CAROLINA ROCHA FERREIRA

Seguros Informáticos: Contributos para uma *framework* de análise de risco a aplicar às ameaças emergentes no setor segurador e empresarial Esfera Legal, Alcance e Potencialidades

Dissertação com vista à obtenção do grau de
Mestre em Direito e Segurança

Orientador:

Doutor António José André Inácio, pela Faculdad de Derecho da Universidad San Pablo CEU, reconhecida pela Faculdade de Direito de Lisboa

Co-orientador:

Doutor José Fontes, Professor Associado com Agregação da Academia Militar – Instituto Universitário Militar

setembro, 2018

"Que seja o eco de uma afronta, o sinal do ressurgir."

Adaptado de "A Portuguesa"

Declaração de Compromisso de Anti Plágio

Declaro por minha honra que o trabalho que apresento é original, e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 25 de setembro de 2018

Agradecimentos

A concretização desta dissertação não teria sido possível sem um contributo especial de algumas pessoas que, durante esta árdua viagem de dedicação, esforço, persistência e coragem, me acompanharam. A todos aqueles que, de forma mais ou menos presente, me assistiram em fases críticas do projeto, agradeço pela paciência.

O ano da conceção deste projeto foi tudo menos fácil, e trouxe consigo a certeza de que quando realmente nos dedicamos a algo, conseguimos ultrapassar os nossos próprios limites e surpreender-nos. Foi um feliz culminar de um grande objetivo.

Em primeira instância, ao meu orientador, Prof. Doutor André Inácio, o meu grande obrigado não só por me fazer acreditar na importância, valor e pertinência deste projeto, como também por se moldar ao meu feitio (nada fácil) e descomplicar tudo aquilo que era simples. Foi preciosa a sua ajuda, acompanhamento e paciência neste ano tão fugaz e preenchido. Obrigada por acreditar em mim, partilhar da ambição, espírito futurista e interesse comum na área da investigação criminal. Por todas as histórias, lições de vida (e profissionais), pela motivação, quando e sempre que necessário, sou-lhe muito grata.

Ao meu co-orientador, Prof. Doutor José Fontes que, apesar da distância e breve contacto, sempre demonstrou a sua disponibilidade, apoio e cujo pragmatismo, profissionalismo e frontalidade foram essenciais para este projeto.

Em segunda instância, à minha família, especialmente aos meus pais, e em particular à minha mãe que, sempre me apoiaram, acreditaram em mim, e me mantiveram em movimento ao longo deste percurso. Os valores que me transmitiram, a confiança e garra que me foi precisa, devo-o a vocês. Faltam-me palavras para descrever a paciência e compreensão em momentos mais tensos e desesperantes, quando nem assim desistiram de mim.

Igualmente fulcrais, foram os meus amigos mais próximos, esses sim que mesmo já sendo insuportável a tolerância para com este projeto e objetivo, nunca me deixaram

vacilar e estiveram sempre lá. Sem eles seria muito mais difícil, já que pela exigência profissional em paralelo, os momentos de exaustão exigiram deles paciência e dedicação a redobrar. O saber ouvir, uma palavra amiga e encorajadora, e um reconhecimento de potencial, foram ingredientes essenciais nesta jornada desafiante.

À Diana, pela amizade que perdura há anos, pelo acompanhamento direto neste projeto e pela paciência incessante a toda a hora. You'll never walk alone.

À Bárbara, Bruna, Rabujas, PPTB, Mica, Cláudia, Maggs e Silvana por todos os desabafos, incentivos, motivações, loucuras e ambição partilhada. Vocês sabem.

Um especial obrigado à Lúcia, que por ser das pessoas que me conhece melhor, desde o início soube que seria capaz de concretizar este objetivo, e esteve sempre lá para mim. Foste incansável, as tuas palavras, apoio e tolerância foram vitais.

A ti, Fábia, um obrigado não chegará para explicar o sentimento de apoio constante, de sugestões desde o início, debates, *brainstorms* e reflexões constantes sobre o tema e sobre a força necessária para levar o barco a bom porto. Mostraste-me como a resiliência se adquire e se incorpora em processos vitais como este, e, em paralelo como ter alguém a nosso lado, com ideais, ambições e força de vontade na mesma vibração, conseguem ser tão brilhantes e estimulantes.

À amiga Ana Paula Ferreira, pelo companheirismo, força, e reconhecimento, que me fez ver que tudo é possível quando se quer, que nunca devemos desistir dos objetivos e acreditar. Obrigada pelos nobres valores e ensinamentos.

A ti, *Amy*, uma cadela muito especial, fiel companheira foste a responsável força motriz e raiz que me manteve empenhada, mesmo sem saberes. A tua garra foi a minha força, e o teu companheirismo sobre tudo prevaleceu. Foste a minha constante e permanente motivação para terminar esta fase, fruto da nossa ligação única e eterna.

Obrigada por tudo,

Carolina Ferreira

Modo de Citação e outros esclarecimentos

1. O modo de citar segue o disposto nas Normas Portuguesas n.º 405-1 e 405-4 homologadas pelo Instituto Português da Qualidade.

2. Os artigos ou partes de livro são citados com referência ao autor, título do artigo ou parte de livro/revista, volume e/ou número, ano e/ou do artigo/livro, quando possível.

3. As monografias são citadas com referência ao autor, título, local de publicação, editora, ano e página. No texto, a partir da segunda citação, é apenas feita referência a autor, título e página.

4. Quanto a obras ou artigos que tenham sido consultados e/ou recolhidos na Internet, a forma de citação será a seguinte: autor, título do artigo, data da publicação, hiperligação da Internet na qual foi obtido e data da consulta.

5. A partir da primeira menção de algum conceito cuja abreviatura/sigla o substitua, o mesmo será utilizado daí em diante pela respetiva abreviatura, quer seja em corpo de texto como notas de rodapé.

6. Nas publicações da autoria de uma instituição, o seu nome vem no lugar do autor.

7. É usado o modo itálico para destacar as palavras escritas em língua estrangeira, latinismos e expressões tipicamente estrangeiras sem tradução direta.

8. As transcrições de textos estrangeiros encontram-se traduzidas para português. As obras estrangeiras foram consultadas na sua língua original e a tradução é da responsabilidade da autora do presente trabalho.

9. Por uma questão de comodidade na leitura, identificam-se, ocasionalmente, as siglas/acrónimos no texto e não apenas na secção dedicada à Lista que se segue. As notas de rodapé englobam informação igualmente relevante, embora apensa ao corpo de texto, por questão de fluidez na leitura.

10. A presente dissertação foi redigida conforme as regras do novo Acordo Ortográfico.

Lista de Siglas, Abreviaturas e Acrónimos

AED – *Agência Europeia de Defesa*

APFIPP - *Associação Portuguesa de Fundos de Investimento, Pensões e Patrimónios*

APP – *Aplicação (por exemplo instalada num smartphone)*

APROSE - *Associação Nacional de Agentes e Corretores de Seguros*

ASF - APS – *Autoridade de Supervisão de Seguros e Fundos de Pensões*

-Associação Portuguesa de Seguradores (antigo **ISP** *– Instituto de Seguros de Portugal)*

CC – *Cartão de Cidadão*

CCTV- *Videovigilância (Closed Circuit Television)*

CEO – *Diretor Executivo (Chief Executive Officer)*

CERT - *Rede de equipas de resposta a incidentes de segurança informática (Computer Emergency Response Team)*

CIMPAS – *Centro de Informação, Mediação, Provedoria e Arbitragem de Seguros*

Cloud – *Serviço de Computação em Nuvem*

CNCS – *Centro Nacional de CiberSegurança*

CNPD – *Comissão Nacional de Proteção de Dados*

CP - *Código Penal*

CPP – *Código de Processo Penal*

CRP – *Constituição da República Portuguesa*

DOS – *Ataque de negação de serviço* (*Denial of Service)*

DPO – *Encarregado de Proteção de Dados (Data Protection Officer*)

EC3 – *Centro Europeu de Cibercriminalidade*

EIOPA –*Autoridade Europeia de Seguros e Pensões Complementares de Reforma*

EM – *Estado-Membro*

ENISA - *Agência Europeia para a Segurança das Redes e da Informação*

EUA – *Estados Unidos da América*

EuroDIG - *European Dialogue on Internet Governance*

FinTech – *Finance and Technology*

FSS – *Forças e Serviços de Segurança*

IAIS- *International Association of Insurance Supervisors*

IoT –*Internet das Coisas (Internet of Things)*

IP – *Endereço de Protocolo da Internet (Internet Protocol)*

ISO - *designa um grupo de normas técnicas/regras que estabelecem um modelo de gestão da qualidade (ou segurança ou outras) para organizações em geral, qualquer que seja o seu tipo ou dimensão. Certifica produtos e serviços, de acordo com as especificações da Organização Internacional de Padronização.*

LC – *Lei do Cibercrime*

LOIC – *Lei da Organização da Investigação Criminal*

LOPJ – *Lei Orgânica da PJ*

NIF – *Número Identificação Fiscal*

OPC – *Órgãos de Polícia Criminal*

PJ – *Polícia Judiciária*

PME – *Pequenas e Médias Empresas*

RC – *Responsabilidade Civil*

RGPD – *Regulamento Geral sobre a Proteção de Dados*

RJASR – *Regime Jurídico de acesso e exercício da atividade seguradora e resseguradora*

RJCS – *Regime Jurídico do Contrato de Seguro*

SI – *Sistemas de Informação*

SIEM – *Security Information and Event Management*

ss. – *Seguintes (referente a artigos seguintes)*

TI – *Tecnologias da Informação (Infraestruturas tecnológicas)*

TIC – *Tecnologias da Informação e Comunicação*

UE – *União Europeia*

UK – *Reino Unido (United Kingdom)*

UNC3T- *Unidade Nacional de Combate ao Cibercrime e á Criminalidade Tecnológica*

Declaração de Conformidade de Caracteres

Declaro que o corpo desta tese, incluindo espaços e notas, ocupa um total de 197.872 carateres para conteúdo principal, e, 47.212 carateres para notas de rodapé.

Declaro ainda que o Resumo utiliza 2042 carateres, e o Abstract ocupa 1971 carateres incluindo espaços.

Resumo

O cibercrime e o risco informático têm vindo a materializar-se sob a forma de ameaças cada vez mais frequentes e cujo alvo são, entre outras, pequenas e médias empresas. Numa ótica de segurança, prevenção e transferência de riscos, este fenómeno associa-se ao mercado segurador, na medida em que os seguros informáticos irão aumentar exponencialmente, fruto da procura e necessidade de uma maior proteção.

Neste sentido, a presente dissertação tem como objetivo facultar uma *framework* de análise de risco a incorporar na avaliação inicial para a conceção de um seguro informático. Para tal, analisou-se as evoluções e investigações já existentes nesta matéria, destacando variáveis de análise sobre o risco informático, e aplicando métricas de vulnerabilidade/tolerância sobre as respetivas dimensões operacionais. Paralelamente, cruzam-se também os aspetos legais e mais recentes diplomas, como o RGPD e a Lei da Segurança no Ciberespaço, com a presente problemática.

Durante o desenvolvimento deste ensaio, verifica-se que a *framework* criada não só funcionará como uma ferramenta auxiliar à compreensão do perfil de risco e dos pontos mais vulneráveis de uma empresa, como também permitirá dar uma resposta ao fenómeno, desde a conceção e escolha de apólices, até à aprovação final da seguradora e celebração de contrato de seguro informático. É ainda pretendido explanar de que forma esta estrutura se incorpora na ótica da empresa e da seguradora, produzindo-se *workflows* de procedimentos e adaptando questionários para este tipo de seguro.

É importante que este tipo de informação seja sempre contemplada aquando de um pedido de seguro informático, na avaliação, cálculo e análise do risco, divulgando a pertinência de tal conduta de modo a evitar infortúnios que tão frequentes são na indústria seguradora, aquando da verificação de sinistros e peritagens técnicas. Pode vir a ser explorado por equipas de peritos e avaliadores/auditores, por entidades de mediação, corretoras de seguros e até departamentos de segurança e/ou consultoria.

Palavras-chave: Seguros Informáticos; Segurança; *Cibercrime;* Risco Informático; Apólice; Empresas; Seguradoras

Abstract

Cybercrime and informatic risk have become more and more frequent threats, targeting small and medium-sized enterprises, among others. From a perspective of risk prevention, risk transfer and security, this phenomenon is associated with the insurance market, as cyber-insurance will increase exponentially, as a result of the demand and need for greater protection.

In this sense, the present dissertation aims to provide a risk analysis framework to be included in the initial evaluation for the design of a cyber insurance. To that end, we analyzed the evolutions and investigations that already exist in this area, highlighting analysis variables on cyber risk, and applying vulnerability / tolerance metrics on their respective operational dimensions.

At the same time, we cross the legal aspects and more recent diplomas, such as the GDPR and the Security in Cyberspace Law, with the object study.

During the development of this project, it will be verified that the framework created will not only function as an auxiliary tool to understand the risk profile and the most vulnerable points of a company, but also to respond to the phenomenon, from the conception and choice of a policy, until the final approval of the insurer and conclusion of a cyber insurance contract. It is also intended to explain how this structure is incorporated in the perspective of the company and the insurer, producing workflows of procedures and adapting questionnaires for this type of insurance.

It is important that this type of information is always included in an application for cyber insurance, in the assessment, calculation and analysis of the risk, disclosing the pertinence of such conduct in order to avoid misfortunes that are so frequent in the insurance industry, when checking claims and technical expertise occur. It can be exploited by teams of experts and evaluators / auditors, by mediation bodies, insurance brokers and even security and / or consulting departments.

Keywords: Cyber-Insurance; Security; Cybercrime; Cyber-Risk; Policy; Enterprises; Insurance Companies

ÍNDICE

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

1. Introdução

As ameaças informáticas emergentes são uma das maiores preocupações da segurança global, sendo que os atores maliciosos, tanto privados como cofinanciados pelo Estado, tendem a avançar, quer seja por ataques violentos ou não violentos, mas maioritariamente por vias virtuais. O risco informático e cibercrime atingem assim o patamar intelectual, industrial e da informação, que é propriedade das maiores potências mundiais, o que se constitui dos maiores desafios à cibersegurança (Skinner, 2014).

Nunca foi tão fácil roubar informação sensível das empresas, atendendo à dependente e crescente necessidade da troca de informações entre companhias, via Internet. A verdade é que tornámos o acesso aos serviços de bases de dados e conetividade tão convenientes para nós, que se tornaram também (demasiado) convenientes para os nossos adversários (Talbot, 2015).

Segundo Bantick (citado por Ralph, 2017)), assistimos a uma grande expansão no escopo da cobertura de interrupção de negócios, que nem sempre é desencadeada por um incidente informático - pode ser devido a uma falha tecnológica. Os clientes (empresas, segurados) estão a tornar-se mais exigentes, e atualmente, grandes empresas procuram adquirir uma cobertura mais ampla que inclua violação de dados, interrupção de negócios e danos à propriedade (intelectual/virtual), por exemplo. Uma área, importante e que raramente é coberta é o dano à reputação que um ataque informático pode causar, pois as seguradoras assumem que a reputação é difícil de medir e, portanto, de segurar.

Da mesma forma, a nível da própria seguradora é pertinente explanar o processamento da celebração de apólices de seguro, a aceitação e avaliação inicial de risco, bem como o tratamento posterior em caso de sinistro informático.

Ainda nesta senda, considerou-se pertinente segmentar o ponto de vista das empresas, na sua gestão interna e análise do estado de cibersegurança, riscos informáticos e ponderação em contratar um seguro informático. Também é destacado o ponto de

vista das seguradoras que, não só estarão perante uma oferta de produto recente e respetivas dificuldades inerentes, como também devem acautelar o seu estado de maturidade referente ao risco informático, conhecimentos técnicos, pré-requisitos e medidas a ter em consideração *à anteriori* de ser assumido um risco desta gama, e de ser celebrado um contrato seguro (Mukhopadhyay *et al.*, 2013).

A presente dissertação de mestrado tem, portanto, como objetivo a definição de um modelo preditivo de análise de risco a aplicar em empresas no contexto de um seguro informático, enquanto contributo para ferramenta a integrar futuramente. A ideia base consiste em promover um roteiro geral para desenvolver um entendimento comum dos termos em que um seguro informático é concebido (fase inicial do processo), e é tratado após um sinistro (fase de averiguação do sinistro). (Kitching, *et. al*, 2014)

É uma investigação que se concentra maioritariamente na análise *à anteriori*, do estado de maturação das empresas, do motivo de interesse por um seguro informático e nas premissas fundamentais para que uma transferência de risco deste tipo se verifique, funcionando da melhor forma.

A escolha do tema justifica-se por se acreditar que a *framework* idealizada seja uma ferramenta fundamental para a sobrevivência das empresas e para o conhecimento de antemão para as seguradoras saberem o que irão segurar, pois quando aplicada corretamente pode detetar qualquer ocorrência de irregularidade, e indicar a maior ou menor probabilidade do risco. Pretende-se também que venha a ser um elemento de pesquisa, alertando para a necessidade e a consciencialização de toda a comunidade, visando contribuir para uma melhor compreensão desta problemática, possibilitando igualmente o aprofundamento dos conhecimentos científicos em matéria da investigação do cibercrime e do risco informático no sentido de aprimorarmos as nossas competências técnicas e práticas nesse domínio, para a segurança de qualquer empresa ou entidade de que sejamos colaboradores.

Assim, porque o risco informático é hoje transversal a qualquer área de negócio, também se pretende obter conclusões relevantes para empresas de todos os ramos,

bem como fornecer um *head's up* às seguradoras, com base na robustez e eficácia da construção de um modelo com estas características. Espera-se, ainda, demonstrar o contributo valioso desta ferramenta no mercado segurador nacional, gabinetes de peritagem, peritos técnicos da área e mitigação antecipada de muitas formas de crime/ataques informáticos na eminência de se verificarem.

As conclusões do projeto vão no sentido da pertinência deste tipo de seguro, não só na tomada de medidas regeneradoras, de prevenção e de modernização tecnológica por parte das empresas, como também em termos de urgência na assimilação e criação de apólices preparadas para um produto deste tipo. A nível empresarial acredita-se ser um potencial produto/ferramenta de crescente procura, o qual se for devidamente implementado e concebido, poderá ter taxas de sucesso e adesão bastante satisfatórias.

1.1.Metodologia da investigação

A presente dissertação segue um design metodológico misto na medida em que se conjugam questões comparativas e correlacionais de forma sequencial, sendo assim abordados aspetos puros de revisão de literatura, de indução, criação e explicação de fenómenos, situado num determinado contexto (empresarial e de seguros informáticos). Do ponto de vista da estratégia de investigação escolhida, esta segue um sistema dedutivo e indutivo, tendencialmente qualitativo, que explora padrões para desenvolver um método de comparação, ou seja, a um nível metodológico trata-se de um método qualitativo/misto[1] (Coutinho, 2013).

Relativamente à caraterização do contexto em estudo, os principais elementos caraterizadores da investigação prendem-se com *inputs* teóricos, processamento e

[1] O propósito da investigação qualitativa é compreender os fenómenos na sua totalidade e no contexto em que ocorrem pelo que o conhecimento do foco do estudo ou problema pode solidificar-se depois de se começar a pesquisa e desenvolvimento do tema, tal como foi verificado.

resultados, pretendendo-se saber como as três dimensões (seguradora, cliente e risco informático) estão conectadas, funcionam e se dinamizam entre si, utilizando a estrutura originalmente prevista. Embora a presente dissertação não seja baseada em resultados estatisticamente precisos, é nossa pretensão, pelo menos, estabelecer um padrão que possa ser útil, examinado e aplicável em futuros casos de estudo (Nelson, 2016).

Quanto ao plano de investigação, esta é uma investigação orientada para o processo de compreender o como e o porquê de determinado processamento de contratação de seguro informático, e a avaliação de risco necessária para tal. Nesta observação qualitativa, a maior parte do tempo foi ocupado no contexto em estudo, por observação de várias realidades semelhantes, com o objetivo de compreender melhor a dispersão do fenómeno. Importa ainda mencionar que o nosso estudo não foi baseado em questões empíricas, mas sim em investigação exploratória neste domínio.

Em termos de procedimento relativo à execução do trabalho, este reveste-se da análise documental, revisão de literatura e princípios básicos da investigação científica. Por forma a se obterem conclusões fidedignas e validáveis, será necessário a interligação entre as várias áreas do saber em estudo, não só no que respeita a apólices de seguros existentes, incorporação de conceitos técnicos e peritagem técnica informática, gestão de risco em empresas, segurança nos negócios e outras polivalências associadas.

Para se compreender o enquadramento conceptual do tema, deve ser entendível que esta é uma investigação qualitativa com abordagem multi-metodológica, já que o campo de análise é muito amplo e difuso. Recorrem-se a técnicas como a análise documental e a triangulação[2], já que uma maior diversidade e integração de métodos, indicadores, *frameworks* e modelos preditivos, produz uma maior confiança e convergência de resultados. Atendendo ao tema e tipo de problemática, é apropriado

[2] Segundo Denzin (1970), a racionalidade desta estratégia reside no facto de se poder atingir o melhor de cada um dos métodos, pois os defeitos de um método são, muitas vezes, os pontos fortes de outro, pelo que a combinação de métodos permite que se ultrapasses certas lacunas específicas.

combinar dois ou mais pontos de vista, fontes de dados, abordagens teóricas ou processos de recolha de dados numa mesma pesquisa, para que se possa obter, como resultado final, um retrato mais fidedigno da realidade e uma compreensão mais completa do fenómeno a analisar.

Pretende seguir uma metodologia do geral para o particular, desde o invólucro do cibercrime e risco informático, até às diversas tipologias criminais por entre as quais se poderão reproduzir estas ameaças virtuais, com consequências na quebra de segurança nas empresas e verificando-se sob a forma de sinistros informáticos. Esta resultará não só de um raciocínio dedutivo e sequencial, com recurso a análise documental, passando pela exploração de textos bibliográficos variados, informações de seguradoras e relatórios das entidades responsáveis do mercado segurador, como também comparação com produtos (contratos seguros) já em vigor em companhias estrangeiras, que se encontram um passo à frente neste produto/sinistro do futuro.

1.2. Formulação do Problema: Contexto, enquadramento, justificação do tema (objetivos e hipóteses)

Decifrando a "árvore de investigação" por detrás da escolha deste tema, deve ser referido que originalmente o rumo seria abordar o terrorismo e o *behaviour profilling* associado. Contudo, fruto da permanente e alucinante atividade profissional, no ramo da peritagem e averiguação de sinistros, considerou-se mais pertinente a junção de *know-how* profissional, com a tão preocupante temática do risco informático, cibercrime e regime estrito da proteção de dados.

A partir daqui, foi feita uma profunda reflexão sobre a pertinência dos seguros informáticos, ainda não afiguráveis na realidade nacional, mas certamente requisitados daqui a breves anos, dadas as necessidades de segurança das empresas e o descorar desta questão ao longo de décadas. Este paradigma é obrigado a mudar, e

com isso, o negócio a evoluir e acompanhar todas as inovações, ameaças e forma de segurança possíveis resultantes deste tão dissimulado inimigo/perigo.

A escolha do tema advém, por um lado, de razões de ordem intelectual que se prendem com o interesse em fundamentar os conhecimentos referentes à importância das fraudes nas organizações seguradoras. Por outro lado, a escolha deste tema decorre também de razões de ordem pessoal e profissional, pois estando a lidar diariamente com sinistros patrimoniais, no ramo de incêndios, furtos e responsabilidade civil, torna-se necessária uma reflexão, pesquisa e o aprofundar de conhecimentos sobre a área de formação inicial, as ciências forenses, cruzando áreas do saber e visando contribuir para a melhoria do futuro do mercado segurador.

O problema desta investigação consiste na validação de uma *checklist/framework* a aplicar enquanto ferramenta para antecipação de risco. Esta problemática derivou de uma investigação preliminar que passou por várias questões que foram surgindo. Desde os sinistros de incêndio, como exemplo a tragédia do país nestes dois anos, e a forma como muitas pessoas ficaram prejudicadas por seguros deficientemente constituídos (seja por infra seguros, seja por indeminizações inferiores aos reais prejuízos) à falta de prevenção nas áreas mais críticas, denotam-se falhas graves na preparação de riscos críticos. Ao se transpor isso para o âmbito da segurança/risco informáticos, que acompanha as evoluções diárias e a constante mutação da ameaça/globalização a este nível, pergunta-se: como estará, se é que está previsto no setor segurador, o assumir de um risco desta magnitude?

Também se constitui como uma questão principal o "como receber o prémio", visto que a seguradora encontra sempre motivos para não pagar com base em incumprimento de uma cláusula algures vigente nas condições contratuais (gerais ou particulares da apólice), isto, de senso comum e noção geral dos segurados. Ora, este tipo de apólice de seguro só será um "negócio" se as contratantes acreditarem nele, logo tem de ser claro, objetivo e sério, e, antes de ser comercializado e apresentado ao cliente, terá de ter uma prospeção, bases sólidas e convenientemente estudadas. Se nos incêndios os lesados ficaram sem património, casas e bens imóveis como pior

cenário, aqui, nos seguros informáticos, poderemos estar a falar de vários clientes (particulares e empresas) afetados, com respetivos dados expostos, ou, empresas comprometidas por ataques informáticos que as levem à falência, ou ainda, custos insuportáveis com manutenção, restauração dos sistemas e reposição da rede de tecnologias de informação. Isto constitui, igualmente, uma tragédia onde, e para a qual, seria agradável ter um seguro informático como apoio.

É uma temática que envolve perceber prós e contras, não só no tecido empresarial, setor da segurança nos negócios como também a segurança informática aplicada a empresas, entre outros. Seja enquanto segurados, clientes, ou terceiros, todos eles têm interesse em saber como funciona na prática um seguro, e se estão devidamente cobertos pelo mesmo, sendo conveniente o entendimento do tipo de riscos que correm, e quais aqueles que pretendem transferir/segurar. Não se trata, assim, de um simples furto de um computador, servidor ou disco externo, mas sim da informação que os mesmos contêm, a quantidade e tipologia de dados armazenados, e a forma como tudo isso poderá comprometer o "negócio" e a confiança junto dos clientes.

Dados todos os assuntos de prevenção falados, tal como incêndios que destruíram casas nas recentes tragédias, muitas seguradoras assumiram perdas totais. Também em casos de vírus como o *WannaCry*, entre outros conhecidos no decurso deste ano, o futuro das empresas fica em jogo. Muitas pagam resgastes de *bitcoins* para reverem os seus dados. Até que ponto custos destes, e de departamentos de informática e engenharia, podem compensar um pagamento de prémio seguro para este tipo de risco?

Estas questões têm se ser exploradas, tanto da ótica do cliente (empresa) como na perspetiva da seguradora, a qual pode vir a vender um produto, cobrar um prémio e submeter uma apólice que cubra danos informáticos vindouros.

Há também um agravamento de risco, não apenas com a evolução tecnológica como pelo desleixo empresarial na manutenção das condições de segurança *on-line*. Devem ser entendíveis as condições a serem obrigatoriamente requisitadas e provadas para ser possível fazer um seguro deste tipo. Não é um tipo de cobertura a que se "possa

dar o luxo" de o seguro ficar mal feito, seja em (des)vantagem para a seguradora ou para o cliente, pelo que entende-se que a análise de risco deve ser condição obrigatória para este tipo de apólice/seguro.

O que se pretende abordar ao trilhar este tema, é, essencialmente, uma consciencialização geral, quer nas empresas como nas seguradoras, sobre os riscos e seguros informáticos, pois a alteração de paradigma obriga necessariamente a uma correta preparação do mercado, antes da oferta, e a uma constante cenarização, planeamento e validação de ferramentas de análise do risco. Tudo isto por inerência do aumento de ataques informáticos conhecidos (fora as cifras negras) bem como ao "apertar de cerca" no que respeita ao tratamento dos dados (Regulamento Geral Sobre a Proteção de Dados, doravante RGPD) e à segurança no ciberespaço (Lei nº 46/2018 de 13 de agosto de 2018).

1.3. Objetivos da Investigação

De forma breve e resumida, identificam-se como principais objetivos desta investigação:

- Explicar a natureza dos seguros informáticos vigentes e emergentes;
- Clarificar do ponto de vista da empresa/cliente e também na ótica da seguradora, os aspetos inerentes à celebração de um contrato seguro desta natureza;
- Analisar os critérios jurídicos envolventes da temática, quadro legal relativo ao direito virtual e dos seguros;
- Relevar o importante papel de uma correta e antecipada avaliação de risco na segurança das empresas, proteção de dados e informações, e contrabalançar com as carências existentes e exclusões que daí poderão advir;

- Gerar contributos ou *guidelines* para a formação de um sistema uniformizador de modelo adequado *(framework)*, que ainda não existe nem está previsto na celebração de contratos seguros para empresas, no ramo informático.

A presente investigação pretende, assim, compreender de que forma se poderá gerar um seguro informático a aplicar a clientes na esfera das PME's, no sentido da sua proteção de dados, prevenção do cibercrime e ataques dos quais possam ser vítimas, numa época desafogadamente digital. Tem também como objetivo, explorar a forma como companhias de seguros deverão aceitar um risco e a que premissas as empresas têm de atender para serem aceites numa futura assunção de risco.

Tratam-se de questões que envolvem elevadas quantias de ativos, não só a montante, em termos de avaliação de risco (valorização de dados de clientes, informações, entre outros) como também a jusante, em termos de prejuízos provenientes de sinistros informáticos, possíveis fraudes e definição de responsabilidades.

Para tal, também será nossa intenção descodificar como se encontra o direito em matéria de seguros e em matéria virtual, bem como a segurança informática das empresas e segurança da informação, face aos novos desenvolvimentos legislativos. Importará, numa próxima investigação, identificar ao detalhe, a forma como a seguradora dará resposta a um pedido de proposta de um cliente para um seguro informático, e o processo de conceção da proposta de seguro, toda a avaliação inicial de risco aquando da mesma, e também ter uma noção de como será o tratamento da peritagem (após sinistro), tendo por base os fluxogramas construídos.

Os objetivos serão, primariamente, qualitativos, no sentido de atingir uma moldura entendível e explicativa de como os seguros informáticos poderão vir a funcionar, na orla nacional onde ainda, se afiguram embrionários, enquanto que noutras nações já estão perfeitamente enraizados. A pretensão será essencialmente dar contributos para um modelo preditivo que as empresas poderão incorporar e deverão cumprir para poderem ter direito a um seguro deste tipo. O valor desta proposta reside na

possibilidade de se gerar uma ferramenta de risco útil e levantar reflexões importantes sobre uma matéria que, por norma, é automática e desvalorizada.

1.4.Estruturação de Capítulos

Esta abordagem investigativa constitui-se por cinco capítulos fulcrais, que embora independentes, se interligam entre si num seguimento concordante:

O capítulo I é referente à introdução, metodologia de investigação utilizada, aos respetivos objetivos da investigação, a formulação do problema e fundamentação do tema, estruturação e limitações encontradas, bem como breve corpo de conceitos.

No capítulo II pretende-se compreender o atual quadro de ciberameaças, enquadrando a problemática da cibersegurança com a área emergente dos seguros informáticos, mais numa perspetiva de estado da arte.

O capítulo III versa sobre o enquadramento jurídico-legal do cibercrime e o direito dos seguros, realçando a importância do regulamento geral sobre a proteção de dados com o qual este tema se cruza. Neste capítulo e subsecções pretende-se, de um modo geral, fazer um enquadramento que nos traga do regime geral da atividade seguradora, enquanto tutelar de riscos, até um quadro mais específico de cobertura de riscos, como é o caso, para os seguros/crimes informáticos. Por forma a ser possível uma fusão entre o sector segurador e a componente informática, terá de ser feita uma ponte com a cibercriminalidade, tipologia de riscos informáticos e compreensão legal das suas vertentes. Opta-se por explorar, assim, os principais diplomas que se referem aos crimes informáticos, uma breve categorização dos mesmos e compreender algumas das lacunas existentes a este nível, pois a partir do momento que existem dúvidas no ordenamento jurídico, as mesmas irão também causar difusão no mercado segurador e nos seguros/sinistros informáticos.

No capítulo IV pretende-se analisar a relação interdependente do cliente/empresa e seguradora, identificando interesses, responsabilidades, vetores modelares e outras

considerações, essencialmente baseado no risco informático e funcionamento/dinâmica central.

Fará, também, sentido enunciar algumas das fraquezas, vulnerabilidades e carências das empresas, no que respeita à segurança da informação, à conservação de dados e ao cumprimento dos normativos mais recentes. Isto prende-se com a necessidade de proteção que sobre as empresas recai e que pode ser uma das forças motriz pelas quais compele a procura por um seguro informático.

Por último, no capítulo V pretende-se formular e sugerir uma *framework* de risco no âmbito dos seguros informáticos, com capacidade para simulação de riscos e projeção de cenários. Esta ferramenta não será testada nem aplicada em caso de estudo, pois carecerá de validações e adaptações em futuras investigações, consoante diferentes variáveis (tipo de seguro, ramo de negócio, riscos da empresa em questão etc). Também se sugerem fluxogramas de modelação para seguimento lógico dos processos em estudo associados.

1.5. Limitações e Dificuldades

Ao longo do tratamento do tema e da própria investigação foram encontradas várias dificuldades, pois trata-se de uma área ainda em exploração a nível nacional, pelo que a informação existente surge maioritariamente de fontes internacionais.

Destaca-se a falta de dados estatísticos, falta de informação sobre o tema, dificuldade da avaliação e gestão do risco, e da própria dinâmica dos seguros, que conta sempre com uma parte de incerteza considerável quanto à mudança, acumulação e verificação do risco. É uma problemática que se reveste essencialmente de uma assimetria/escassez grave de informação, seleção adversa e falta de estudos e explorações sobre o fenómeno. Tudo isto complicou a investigação e recolha de dados fidedignos, tornando o estudo mais moroso. Contudo, contribuiu

indiretamente, para a criação de algum espírito crítico, adaptação, extrapolação, raciocínio indutivo e autonomia, por forma a ser dada opinião e nos pronunciarmos em concreto sobre uma área ainda em desenvolvimento e tão pouco falada.

Também o tema em si é muito amplo, e facilmente tendeu a dispersar, seja pela vastidão do mundo digital, polivalência criminal, entre outras, tendo sido necessária a constante restrição ao puramente essencial, centralizado nos seguros.

1.6. Corpo de Conceitos

Os principais conceitos de referência para o lançamento desta investigação revestem-se essencialmente de vocabulário próprio da atividade seguradora, algumas (residuais) componentes técnicas, e variantes associadas ao risco e setor informático. Assim, enquanto parte da harmonização conceptual, destaca-se:

Ameaças: Conceito que sempre se verificou e, pode gerar consequências negativas nas operações da empresa. Comummente são classificadas como ameaças: a) a facilidade de acesso às instalações; b) desastres ambientais; c) falhas e acessos não autorizados; d) uso inadequado de *software*, etc. Temos ameaças de carácter físico como uma inundação, e, ameaças de carácter lógico, como um acesso não autorizado a uma base de dados.

Apólice: Contém desde: a) nomes; b) dados; c) assinaturas; d) a designação do objeto seguro; e) a natureza dos riscos garantidos; f) a partir de que momento se garantem os riscos e por que duração; g) o capital seguro; h) o prémio e outras cláusulas que aparecem na política de acordo com as disposições legais, bem como as legalmente acordadas pelas partes contratantes (González, 2017).

Ataque Informático: Série de atos que consistem no uso ou operação de qualquer sistema de computador, por/através de qualquer pessoa ou grupo (s) de pessoas, seja agindo sozinho ou em nome de / ou em conexão com qualquer organização (ões), e,

se induzida (ou não) pelo uso de força ou violência de ameaça da mesma para cometer tais atos, o que resulta num compromisso de segurança que se destina a concretizar uma quebra de rede (BritInsurance, 2017).

Ativos: São aqueles relacionados com os sistemas de informação: dados, serviços, documentos, edifícios, hardware/software, recursos humanos, etc (Tenzer & Sena, 2004).

Contrato Seguro: Aquele que a seguradora o obriga mediante a cobrança de um prémio serve para o caso de acontecer algo e, cujo o risco é objeto de cobertura a indemnizar (dentro dos limites contratuais), verificado pelo dano provocado ao segurado ou prejuízos resultantes. Estipula as condições gerais e particulares, e estabelece um vínculo contratual cliente-seguradora (Pereira, 2013).

Crime Informático: **S**erá "um qualquer ato ilegal onde o conhecimento especial de tecnologia de informática é essencial para a sua execução, investigação e acusação.", sendo "uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre com a utilização de dispositivos habitualmente empregados nas atividades de informática". Também considerado "aquele perpetrado contra bens jurídicos computacionais e conjunto de dados/informações contidos nos sistemas informáticos, estando estes armazenados, sob manipulação ou em transmissão ". O crime informático é todo o crime que seja praticado com recurso a meios informáticos - qualquer conduta criminosa que na sua realização faça uso da tecnologia eletrónica, seja como método, meio ou propósito (Neto, 2003) e (Gómez, e Espinosa, 2014).

Franquia: É algo bom tanto para a seguradora (reduz custos, despesas de gestão, frequências de acidentes) como para o segurado (estimula as medidas de prevenção, proteção e natureza organizacional interna que não pode ser realizado sem a existência de franquia / dedutível). Por norma trata-se do valor contratual que fica definido como sendo assumido pelo segurado, em caso de sinistro (Fernándes,2007).

Fraude: Premeditação de ação, com objetivo de obter vantagem de contrato de seguros a partir de ocorrência inexistente ou planeamento de um sinistro. Frequência menor, mas valores envolvidos maiores. "Qualquer ação ou omissão realizada com o propósito de ilegitimamente obter uma vantagem, patrimonial ou não patrimonial, quer para o indivíduo que a comete, quer para um terceiro, punível por lei, regulamentos ou normas internas, constitua ou não ilícito criminal" (Fraguio & Macías, 2011) e (Pereira, 2013).

Gestão de Riscos: Designação de "um processo realizado pelo Conselho de Administração de uma entidade, a sua gestão e restante pessoal, aplicável à definição de estratégias em toda a empresa e concebido para identificar potenciais eventos que possam afetar a organização, gerir os seus riscos dentro do risco mínimo (aceitável) e fornecer segurança razoável sobre a realização dos objetivos" (Aranceta, 2007).

Impactos: Consequências da ocorrência de distintas ameaças, que são sempre negativos. As perdas geradas podem ser financeiras, ou outras, e de curto ou longo prazo (Tenzer & Sena, 2004).

Lesado: Pessoa/Empresa que sofre o prejuízo patrimonial e não o proprietário/utente dos dados ou programas informáticos. A lesão do património enquadra-se na utilização de meios informáticos e intromissão nos sistemas onde os dados estão presentes, nos quais está subjacente alguma forma de fraude que tenha como intuito obter enriquecimento ilegítimo. Lesado também afigura danos corporais ou morais (Azevedo, 2016).

Miniaturização: Refere-se à inovação e evolução tecnológica em equipamentos cada vez mais pequenos e sob a forma de itens facilmente portáteis com capacidades informáticas de grande alcance e monitorização. Este conceito verifica-se por exemplo em captações de conversas telefónicas a quilómetros de distância, colocação de microfones em computadores, detetores de fumo, ou qualquer objeto presente num escritório ou habitação, que torna viável a captação/recolha de informação da mais variada ordem (Muravska, 2013) e (Bressler, 2014).

Risco: Define-se como aquela eventualidade que impossibilita o cumprimento de um objetivo. No que respeita à tecnologia, o risco surge como a probabilidade de uma ameaça se concretizar, devido à existência de vulnerabilidades, ao valor estratégico do alvo, e à capacidade de concretização do ataque (Tenzer & Sena, 2004).

Sinistro: Ocorrência súbita e imprevista, de caráter acidental, intencional ou negligente, que faz funcionar a ativação de, pelo menos, uma das coberturas da apólice de seguro. Resulta em danos materiais, corporais e/ou outros prejuízos. O sinistro corresponde à verificação, total ou parcial, do evento que desencadeia o acionamento da cobertura do risco prevista no contrato. A sua verificação deve ser comunicada ao segurador pelo tomador de seguro (art.99 e 100º do RJCS).

Sistema informático: Sistema informático, segundo o art.º 1º alínea a) da Convenção de Budapeste, é um equipamento ou conjunto de equipamentos interligados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o tratamento automatizado de dados.

Vulnerabilidades*:* Certas condições inerentes aos ativos de uma empresa, através das quais as ameaças se concretizam. Derivam da falta de conhecimentos do utilizador, tecnologia arcaica, antivírus desatualizado, etc. "A vulnerabilidade é determinada, até certo ponto, por parâmetros específicos da organização, como tecnologia, processos e pessoas. Ela é caracterizada por um componente de risco idiossincrático que, para uma seguradora, representa o risco de risco moral. Devido ao caráter público dos investimentos em segurança de TI, ou seja, o nível de segurança de uma empresa depende das medidas de segurança de outros parceiros na cadeia de suprimentos, as empresas tendem a investir menos do que seria ideal para a sociedade (Eling & Schnell 2016).

2. Relação entre o Quadro de Ciberameaças e a Globalização

2.1.A Globalização e a Sociedade da Informação

No extenso e mutável universo do Direito e da Segurança, as constantes e emergentes ameaças são alvo de preocupação e foco quer seja para os Governos e legisladores, como também para as Forças e Serviços de Segurança, doravante FSS. É evidente a pertinência, e urgência, da temática em redor da globalização e das ciberameaças, dada a expressão crescente de fenómenos criminais complexos de que somos público, e alvo, e que também nos acompanha na presente sociedade de risco a nível empresarial.

Na sociedade global atual o Estado enfrenta um conjunto de ameaças diversas, consequência de um ambiente marcadamente afetado pelos desenvolvimentos políticos, económicos, sociais e tecnológicos. Um ambiente em que os riscos existentes têm o potencial de desarticular as infraestruturas que suportam a nossa sociedade. Esta realidade demonstra que a segurança hoje, mais do que nunca, se encontra no centro das preocupações do Homem (Fiães, 2005).

A ameaça constante, intermitente, instável, súbita e imprevista a que daremos enfoque ao longo desta dissertação, trata-se da ciberameaça ou mais concretamente, da percentagem dos riscos que possam advir da utilização de meios informáticos ou tecnologias da informação, de ora em diante denominadas de TI's. Esta ameaça deriva, não exclusivamente, da globalização que é geradora do sentimento de insegurança, mas também devido à maior qualidade técnica e sofisticação das operações criminosas (Marine, 1999) e (Pereira, 2017 a).

Ao contrário dos crimes convencionais, o crime informático raramente é reportado às autoridades por parte das empresas, mesmo quando há dados perdidos, seja pelo receio de sofrer represálias ou de perder mercado, deixando muitos casos no desconhecimento, o que limita a investigação criminal. O facto de existirem oportunidades para este tipo de crime se concretizar, obriga a que o mercado seja

recetivo aos mesmos – na deteção e comunicação - contando sempre com algumas lacunas do aparelho policial, e a natural corrupção implícita das redes (Pereira, 2017).

Este tipo de crimes apenas chama a atenção das forças policiais quando tem impactos elevados e amplamente difundidos. É certo que não está previsto o combate a esta criminalidade de forma preemptiva, contudo a prevenção criminal neste âmbito ainda pode ser bastante melhorada. Destaca-se a análise de provas digitais e filtração de elementos recolhidos na investigação como sendo um processo moroso cuja entidade nomeada e competente para o seu tratamento – Polícia Judiciária, doravante designada por PJ - não dispõe de meios suficientes e disponíveis para dar resposta, em tempo útil, a todos os processos em curso, apesar de contar com apoios externos tais como entidades que realizam perícias informáticas (Azevedo, 2016).

Importa também mencionar que existe uma tendência para simplificar e subvalorizar em demasia a constante ameaça, sendo muitas vezes mal interpretada, por não ser tão direta a compreensão da causa-efeito. A ameaça representada é muito mais permeável e grave do que uma simples penetração de antivírus ou desbloqueio das proteções de um computador ou servidor. Falamos aqui em grande escala, em termos de riscos letais para empresas, dados e informações comprometidas, entre outros. A repercussão desta criminalidade reflete-se, na maioria, em pequenas e médias empresas, de cariz privado, tendendo a ocorrer por desleixo dos mecanismos de controlo e proteção das TI, contaminação gradual das mesmas e sistemas arcaicos com estruturas frágeis (Marine, 1999) e (Pazmiño *et al*, 2017).

Compreende-se, portanto, o atual quadro de ameaças à segurança, onde as novas tecnologias da informação estão a introduzir-se de forma vertiginosa na nossa vida. A irrupção destas tecnologias no mundo empresarial tem propiciado o surgir de novos modelos de contratos e formas de contratação. Aqui entrarão também, em breve, a contratação de seguros informáticos, matéria ainda embrionária em Portugal. O ordenamento jurídico não pode ficar à margem desta situação pois a velocidade com que avança o mundo virtual, não tem sido acompanhada com o avanço da regulação jurídica desta matéria (Arien, 2003).

Neste seguimento, surgiu recentemente – maio 2018 - o Regulamento Geral sobre a Proteção de Dados[3] o qual revela algumas desigualdades de tratamento, nomeadamente no que respeita ao regime das penalizações, entre entidades públicas e privadas. Este diploma regula a forma do tratamento de dados pessoais e a livre circulação desses dados, especialmente para empresas, sendo que desde a sua publicação fez notar o quanto irá ter impacto nos vários departamentos de uma qualquer organização, seja da administração pública ou particular. O mesmo prevê um regime de contraordenações para o seu incumprimento, bem como a tipificação de comportamentos como crime, com respetivas sanções penais, pelo que será alvo de especial atenção no decurso da presente investigação (Gomes, 2017).

Face ao exposto, o uso de dados/informações e a maioria dos serviços que utilizamos, seja dentro ou fora do ciberespaço, compilam e armazenam dados pessoais. A maioria dos sites que visitamos não têm padrões básicos de privacidade, motivo pelo qual muitas vezes dados são capturados sem autorização, e vemos os nossos interesses a serem coligidos do mundo virtual e nós alvos da correlação de informação a que, ingenuamente e naturalmente, acedemos. O risco é por isso crescente, na proteção de privacidade e identidade, o que se tornará cada vez mais alarmante para utilizadores sem capacidade técnica e *know-how* (Rogerson & Pease, 2004).

Vivemos num mundo dominado pela máquina, num real ciberambiente, onde a sociedade nos parece circundar a rede, com a forte dependência da "máquina" e dos sistemas, o que atesta esta pretensão que se vem a verificar desde idades precoces e nas camadas mais jovens. Estamos a passar de uma Internet de pessoas para uma Internet de coisas – *"Internet of things"(IoT)* – que se adjudica à "miniaturização das coisas", conceitos ambos criados para a revolução tecnológica em que os dispositivos estão conectados à Internet[4] (Gubbi *et al* ,2013). Pensamos, vulgarmente, nos computadores ou *smartphones*, mas hoje em dia existe uma oferta imensa de

[3] Segundo o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).
[4] O IoT diz respeito ao novo paradigma tecnológico concebido como uma rede global de máquinas e dispositivos capazes de interagir uns com os outros (Azevedo, 2016) e (Lee,2015).

utensílios que se encontram conectados à Internet, via GPS ou outros, como é o caso de alguns eletrodomésticos, pulseiras que registam a atividade física do utilizador, e tantos mais (Muravska, 2013), (Amaral, 2014) e (Lee, 2015).

Por sua vez, o uso da tecnologia facilita muitas tarefas diárias, torna mais fácil a comunicação, automatiza tarefas, permite realizar negócios on-line e de forma mais intuitiva, entre outras atividades. No entanto, na maioria dos avanços na ciência, a tecnologia também está a ser utilizada para cometer atos ilegais, tal como os crimes informáticos. Atualmente as informações e dados armazenados nos equipamentos informáticos são inseguros, e convertem-se em milhões de dólares por parte das empresas, a fim de proteger os ativos mais preciosos: a informação (Gómez e Espinosa, 2014) e (Gomes, 2017).

Nesta senda, entende-se que com a evolução da tecnologia têm também surgido novos tipos de dados que não poderiam ser tratados com recurso às tecnologias habituais de manuseamento da informação, o que levaria os gerentes empresariais e utilizar grandes volumes de informação como ferramenta para assegurar o tratamento de dados nas diferentes áreas do negócio. Isto traz preocupações com ameaças relacionadas com pedidos de resgate de informação, com pagamentos através de criptomoedas (situação a que várias empresas já se viram sujeitas nos últimos anos), entre outras consequências nefastas para a organização. Por este motivo, nos debruçaremos mais adiante sobre esta problemática, e por que motivos deve ser minuciosamente analisada de antemão a contratação de um seguro para "minimizar" os prejuízos de tamanho risco (Pazmiño *et al.,* 2017) e (Bacelar, 2018).

Deste modo, entende-se a importância de se debruçar sobre a prevenção, atendendo à amplitude da ameaça desta tipologia criminal, e que aqui relacionaremos com o setor segurador, por intermédio dos riscos informáticos.

2.2. Problemática da Segurança, Cibercrime e Seguros

No seguimento do raciocínio anterior, sobre as novas ameaças que se verificam, importa relevar que os crimes informáticos, não se tratam de novas ameaças, no sentido lato. Estas sempre se verificaram, com a única diferença que, presentemente, "o que é novo é a sua intensidade, potencial de impacto e o consequente risco que representam para os Estados e para as sociedades. Esta realidade obriga a uma nova reflexão sobre a segurança", pois no recente quadro de ameaças, riscos e oportunidades, a dúvida que se coloca é quando seremos atacados e não se vamos ser atacados (Fiães, 2005).

Enquanto profissional da área, fruto da convivência ambivalente com a seguradora (a montante) e o cliente/segurado (a jusante), é possível ter uma visão holística do cenário prático onde se verifica a manifestação do risco, quer seja por consumação de crime (ex. furto ou roubo), por verificação do risco, ou como mero acidente súbito e imprevisto (ex. incêndio ou explosão). Contudo, pela formação focada na investigação criminal, direito penal, segurança e seguros, há um denominador comum que apesar de pouco explorado até à data, sobressaiu em reflexão interna, e se crê vir a constituir uma problemática de segurança, também a nível da oferta: os seguros informáticos. Neste seguimento, será relevante debruçarmo-nos sobre esta matéria que abarca uma espécie de fusão entre os produtos vendidos (apólices de seguros) e respetivas coberturas, bem como os riscos, ameaças e inseguranças associadas. Tudo isto abarca três pilares em comum: a segurança, o cibercrime/riscos informáticos e os seguros.

Na ótica da segurança, esta constitui um valor instrumental não absoluto, um valor de garantia e uma condição de realização da liberdade. Quando se fala de segurança tem de se pensar na vertente interna e externa, mas, no seu geral, esta deve ser multinível e transversal. Por vezes, as ameaças mais afastadas geograficamente

poderão ser aquelas dignas de maior preocupação, o que valida uma ação da segurança numa linha primariamente exterior (Garcia, 2006) e (Bacelar, 2017).

A crescente sofisticação dos equipamentos e tecnologia, associado à capacidade técnica empregue para comprometer usuários, causa interrupções nas comunicações, ou pode levar ao furto de informações que comporta um elevado risco para o negócio. Na mesma proporção, quando se diminui os níveis de segurança, as vulnerabilidades ampliam-se e intensificam-se (Inácio, 2017) e (Pereira, 2017 a).

De facto, os riscos são crescentes e não é possível ser dada uma medida direta da perda, estando aqui em jogo redes completas comprometidas, e centenas de milhares de ficheiros extraídos. Este tipo de ameaça tem, nos dias que correm, um potencial de custar à economia mundial biliões de dólares entre outras perdas imensas noutros setores (Power & Forte, 2007) e (CSIS, 2013).

No que alude aos crimes informáticos, maioritariamente focados a nível corporativo e no tecido empresarial, há que reportar à projeção do fenómeno, que assumiu desde formas arcaicas até métodos sofisticados, onde, por vezes, é quase impossível fazer um rastreamento da "pegada digital" deixada pelos autores. Por este motivo, tem-se tornado incrivelmente fácil realizar atos de espionagem informática[5] neste contexto, pois as organizações têm utilizado a tecnologia para elevar as suas operações, estando muita informação pessoal e empresarial disponível, por vezes exclusivamente, na sua forma eletrónica, e sujeita em grande carga ao risco informático (Jones & Jones, 2008) e (Santos, 2017).

[5] O crime, inicialmente revestia-se de um roubo de ideias, por meios físicos e mais diretos dos que atualmente é possível perpetuar por via virtual. No entanto, a recolha de informação privilegiada e dados competitivos sempre foi ambicionada pelas vantagens que se pode retirar ao nível de vendas, mercados, clientes e aumento de lucros. Tem-se, assim, assistido a uma mudança radical do ambiente da informação, o qual, sendo de uma dimensão agora empresarial e organizacional, em ambientes com menos papel e com recurso a mais dispositivos tecnológicos, vê a sua configuração tradicional transformada. Tudo se resume a um conflito de interesses (Bressler, 2014).

Muitos autores por detrás dos crimes informáticos, não só se tornaram internacionais no seu alcance como também exibem um grau de flexibilidade e adaptabilidade em métodos que representam desafios consideráveis para as FSS, serviços de informações e à sociedade no seu geral. Um dos maiores desafios é a urgente necessidade de gerir os riscos, matéria transversal a outras áreas, veja-se o que aconteceu nos incêndios de 2017, onde a prevenção que revelou falhas, tornou-se fatal. Contudo, importa referir que grande parte das companhias de seguros em conjunto com a Associação Portuguesa de Seguros/Associação de Supervisão de Seguros e Fundos de Pensões (adiante APS – ASF) tomaram uma posição solidária e condescendente, apoiando os segurados tanto quanto possível, facilitando a gestão e regularização dos processos de sinistro, porquanto se tratar de situação de cariz excecional (McCulloch & Pickering, 2009).

No seguimento desta situação, compete, igualmente, alertar para o facto de uma parte dos proprietários nacionais esperar pelo apoio estatal em vez de cobrir os seus investimentos, industriais ou agrícolas, de forma consentânea com apólices adequadas. Esta opção mostrou-se principalmente traiçoeira no ramo de habitação.

Nesta senda, os ataques informáticos preocupam as corporações nos departamentos executivos e de segurança que lidam com questões de espaço virtual e de TI, havendo pesquisas que revelam que mais de 60% das empresas têm vindo a classificar o risco informático como sendo altamente prioritário. Este risco é um risco de toda e qualquer empresa, não se tratando (há muito) de uma simples ameaça informática. Avassala barreiras e fronteiras, ameaça a reputação de empresas, a resiliência das suas cadeias de fornecimento, causa danos a terceiros, entre outros resultados nefastos para o negócio ou indústria em causa (Santiago, 2016).

É altamente provável que, se verifique no seio de determinados negócios, Administração Pública ou entidades com dados confidenciais de clientes, a ocorrência de ataques informáticos dos quais serão, ou irão constituir-se como alvos.

As soluções nesta ótica da segurança não serão baratas aos olhos dos investidores, administração das empresas e capacidade do orçamento interno das mesmas (Gomes, 2017).

Contudo, a segurança informática deve ser posta em primeiro lugar da lista de prioridades, como elemento fundamental para o êxito do negócio, pois, o que se julga ser um risco razoável e pouco provável, pode muito bem tornar-se o risco máximo e acarretar o sequestro de ficheiros, a paragem de sistemas de produção entre outros danos que trarão prejuízos para os pequenos, médios e grandes empresários. Desde uma sensibilização dos funcionários e colaboradores, à exposição das fragilidades junto dos CEO's[6], deve ser um ativo estratégico nos objetivos de qualquer empresa (Muravska, 2013) e (Bressler, 2014).

É, assim, fácil de compreender a existência de um armazenamento massivo de dados, nas empresas. Neste sentido, e tal como referido por Bressler (2014) "importa ter a consciência que proteger um negócio e respetivas propriedades intelectuais, pode ser um desafio complicado, pois as empresas necessitam entender que qualquer negócio é vulnerável e que os dados mais preciosos e sensíveis devem ser guardados de modo seguro". Contudo, esta gestão de dados constitui-se como um enorme problema quando não se tem um método adequado para o processamento de informação, pois as empresas acabam por dissipar potencial, que poderiam estar a aproveitar (Pazmiño, *et al* 2017).

Afigura-se necessário que as empresas se comecem a preocupar com riscos que não conseguem controlar, quer sejam aqueles que um responsável de segurança informática com o seu departamento não consigam proteger em toda a frente, ou, aqueles que apesar de garantir todos os ideais de segurança em vigor, acabarão inevitavelmente por acontecer, e sofrer as consequências, pois diariamente existe uma sujeição a diversos e mutáveis riscos (noção de risco mínimo). As empresas líderes

[6] Ainda relacionado com as ciberameaças e riscos para a atividade empresarial, deve ser tida em consideração a segurança dos sistemas informáticos e da informação, para a prevenção de uma qualquer tentativa de acesso indevido. Os riscos devem ser observados, maioritariamente por ameaças externas, mas, também por canais internos e do mapa de pessoal de cada empresa, começando pelos CEO's (Inácio, 2017a).

de mercado, com segredos comerciais poderosos, ou com dados cuidados de clientes com influência, tornam-se alvos preferenciais, o que por sua vez irá levar à consciência das administrações e à reflexão interna futura de querer salvaguardar um risco, que por si só internamente não é possível acarretar (Crane, 2005).

Será a partir daqui que surgirá o ímpeto para recorrer ao mercado segurador em busca de soluções, apoio e produtos que se adaptem às necessidades (primordialmente informáticas, que são as de mais difícil contingência), perda, furto ou resgaste de dados, e também a eventual paralisação do negócio por via virtual. Naturalmente, o mercado segurador deverá estar capacitado para corresponder às expectativas e ter oferta multifacetada para escolha do cliente.

O crime informático, pode verificar-se sob os mais diferentes tipos de risco informático, e, cada ilícito, pode, por sua vez, derivar em inúmeros *modus operandi*[7], cujo agente é comummente caraterizado por *hacker*[8] que se constitui a personagem criminosa deste mundo virtual. Por todo o risco oponível às empresas, deverá haver uma política de *acountability* e uma gestão/mapeamento dos riscos em cada organização, o que transversalmente e num futuro próximo, passará também por uma "fusão" da cibersegurança com os seguros – *cyber insurance*[9] *(*Veiga & Dias, 2010) e (Dias 2012).

Incorporando agora o tema matriz dos seguros, o mesmo prende-se com um novo paradigma do sector da banca e seguros, onde é necessário alertar para os aspetos suprarreferidos, e tantos outros que surgirão pela globalização e alteração do paradigma criminal e do risco informático. Isto levará à necessidade da

[7] *Modus operandi* refere-se ao modo de atuação na prática do crime, a forma como o ilícito criminal se pode verificar ou concretizar, i.é, no objeto em estudo, a forma sobre a qual se consuma o risco informático.
[8] Estes acedem, sem autorização dos seus legítimos titulares, a computadores, sistemas e redes informáticas ou telemáticas alheias. No meio dos cibercriminosos é sagrada a distinção entre *hackers* e *crackers*, pois os últimos têm como objetivo a corrupção e quebra dos programas informáticos, apagar informação ou tornar um sistema informático (ou mesmo um local) inoperacional/inutilizável.
[9] O seguro informático (*cyber insurance*) é frequentemente discutido como uma grande oportunidade de mercado por causa da alta consciencialização do público em relação a este risco, e a crescente exposição ao mesmo (Biener, 2015) e (Eling & Wirfs,2015).

consciencialização das seguradoras, instituições bancárias e também das empresas que contratam seguros, ou o pretenderão fazer num futuro próximo.

O sector segurador abarca um enorme fluxo de informação, várias carteiras de clientes onde residem dados confidenciais tais como moradas, detalhes da constituição de objetos seguros sejam eles casas, carros, outros bens ou patrimónios. No alucinante mercado competitivo, e com a elevada taxa de sinistralidade com que se debruçam, a maioria das companhias de seguros estão focadas na satisfação do cliente, no bom serviço prestado, no valor das indeminizações em jogo e nos prazos praticados.

Contudo, são descoradas as avaliações de risco, principalmente aquelas que inicialmente deveriam ser feitas antes da conceção dos contratos seguros. Em boa verdade, as seguradoras por vezes apenas têm a real noção do que estão a segurar e da respetiva envolvência, quando ocorre um incidente e é participado o respetivo sinistro. Isto não poderá, de forma alguma, suceder num eventual seguro informático, dado que uma avaliação inicial do risco, o conhecimento integral do objeto seguro e a definição das circunstâncias ao momento do contrato, têm de ser rigorosamente avaliadas (San José-Marti, 2013).

Segundo notícia lançada pela TSF[10], as alterações climáticas fazem as empresas de seguros antecipar uma mudança nos seus contratos, mas, acima de tudo, despertam uma maior atenção dos clientes em relação às matérias cobertas pelos seguros. Assim, acredita-se que não só as alterações climáticas como também as alterações tecnológicas, venham a mudar os seguros, o que remete para uma alteração de paradigma. De igual forma, e na mesma proporção se antevê panoramas diferentes de sinistros, no ramo virtual e empresarial, aos quais será necessário prestar a devida atenção, na ótica da antecipação do risco informático, formação neste sentido, sensibilização da ameaça e preparação das partes envolvidas.

[10] "O presidente da Associação Portuguesa de Seguradores também alerta que é cada vez mais importante, os cidadãos e as empresas, atualizarem os valores segurados, para que eles possam acompanhar valorizações ou desvalorizações do património". Retirado de "As alterações climáticas vão mudar os seguros?" TSF Rádio Notícias, publicado a 29 de janeiro de 2018.

Uma outra ressalva pertinente, trata-se do contrabalanço entre o risco mínimo e o risco razoável (ou residual), que deve ser tido em equilíbrio entre a seguradora e o cliente para que seja possível uma junção de interesses e um consenso quanto à matéria em risco e ao objeto a segurar. Neste sentido, é pertinente compreender as fragilidades associadas à recolha de informações, do seu ponto de vista ético e legal, indo ao detalhe da diferenciação entre métodos, condutas e abordagens do fenómeno (Watkins, 2014) e (Bacelar, 2018).

Uma vez feita esta imprescindível análise de conceitos iremos de seguida apreciar em concreto, os regimes legais concernentes ao mesmo, bem como um enquadramento jurídico no que respeita à atividade seguradora e diplomas legais associados ao cibercrime/riscos informáticos.

3.Enquadramento Jurídico-Legal Do Cibercrime e o Direito dos Seguros

3.1.Direito dos Seguros

Para que seja possível abordar a temática dos seguros informáticos é fulcral explorar a regulação jurídica da atividade seguradora, pois só assim se conseguirá integrar as questões de cariz penal e criminal dos ilícitos informáticos. Com efeito, resultante do enorme eclodir do universo informático e da relevância que os computadores assumem no dia-a-dia, é indesculpável o descuido com que os juristas incorrem nesta matéria, seja por indiferença ou desconhecimento. Com isto, surgiram outras problemáticas acessórias em torno dos riscos informáticos e a garantia que é necessária em parceria com o sector segurador, o que torna a busca por soluções legais, uma tarefa ainda mais difícil e exigente (González, 2017).

O Regime Jurídico de Acesso e Exercício da Atividade Seguradora e Resseguradora (doravante denominado por RJASR), diploma base e de maior expressão, consta da Lei nº147/2015 de 9 de setembro, e aprova o regime processual aplicável aos crimes especiais do setor segurador e dos fundos de pensões, e às contraordenações cujo processamento compete à Autoridade de Supervisão de Seguros e Fundos de Pensões[11]. A ASF-APS[12], segundo os termos do Regulamento (UE) n.º 1094/2010, do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, é a autoridade competente para o exercício da supervisão e coopera com a *European Supervisory Authority for Occupational Pensions and Insurance* (EIOPA) para os efeitos previstos no RJASR. Presta também à EIOPA informação sistémica ou pontual

[11] Note-se que o sector dos seguros envolve a banca e seguros, mas também os fundos de pensões, motivo pelo qual houve uma re-nomenclatura do Instituto de Seguros de Portugal, passando agora a intitular-se Autoridade de Supervisão de Seguros e Fundos de Pensões - Associação Portuguesa de Seguradores (ASF-APS).

[12] Esta entidade tem por objetivo promover a solidez e estabilidade financeira de todas as instituições sob a sua supervisão, zelando pelo cumprimento de princípios, regras e boas práticas que garantam a manutenção dos bons padrões de conduta por parte dos operadores neste mercado. Visa definir orientações a prosseguir na política para o sector segurador e atividades conexas no âmbito das seguradoras, fundos de pensões e mediação. Tem ainda competências de *enforcement*, relações internacionais e institucionais, seguindo vários princípios regulatórios, gestão de fundos, patrimonial e outros recursos (retirado de Plano de Prevenção de Riscos de Corrupção e Infrações Conexas do ISP (9 de junho 2010, Conselho Diretivo)

necessária à execução de funções[13]. Este é um regime que se aplica a empresas de seguros, bem como às suas sucursais e também a sociedades gestoras de participações neste setor, com sede em Portugal, e que pretendam exercer atividade na UE, regulando as condições de acesso e exercício, bem como a sua supervisão, recuperação ou liquidação (artsº 1 e 2).

Por entre várias definições e conceitos que explana, destaca-se o de "Estado membro em que se situa o risco" dado que, no crime informático e sinistros de ramo informático torna-se difícil compreender, em concreto, qual a origem do risco bem como a sua localização. Ainda que uma empresa esteja sedeada num determinado local e seja esse o local de risco estipulado na apólice, não deixa de ser importante ter em atenção este conceito por contraponto com o direito virtual, onde se esbatem as fronteiras, e o risco é amovível no que respeita aos dados, informações em rede, e riscos informáticos[14] (Verdelho, 2003).

Os membros dos órgãos da ASF-APS, as pessoas que nele exerçam ou tenham exercido uma atividade profissional, bem como os auditores e peritos mandatados por esta autoridade, estão sujeitos ao dever de sigilo profissional. Nesta senda, o dever de sigilo torna-se imprescindível pois será de prever que o perito/técnico para analisar o sinistro/incidente informático, tenha de lidar com informações confidenciais e esteja incumbido de preservar as mesmas[15] (Art.º 32º, nº 1 do RJASR). São também referidos neste regime os ilícitos penais (art.º 356º e ss.), a desobediência (357º), as penas acessórias (358º) e as contraordenações (359º) a aplicar às empresas do ramo.

[13] Neste seguimento será pertinente mencionar ainda a IAIS (*International Association of Insurance Supervisors)*, estabelecida em 1994, sendo uma organização de associação voluntária de supervisores e reguladores de seguros, com mais de 200 jurisdições, constituindo 97% dos prémios de seguro do mundo. Visa promover uma supervisão eficaz e globalmente consistente do setor de seguros, a fim de desenvolver e manter mercados de seguros justos, confiáveis e estáveis para o benefício e proteção dos segurados.

[14] Os crimes informáticos dirigem-se tendencialmente contra interesses patrimoniais (ex. burla informática ou direitos de autor), contra as pessoas (crimes contra a honra ou pornografia de menores) e contra dados e informação (falsidade informática, acesso ilegítimo, acesso indevido, sabotagem informática, danos informáticos, etc.). Este último tipo de crime (contra dados) constitui aquele compatível com os princípios da segurança informática – confidencialidade, disponibilidade e integridade (Bernal, 2009).

[15] Para auxiliar numa melhor compreensão do suprarreferido deverá consultar o art.º 34º do presente regime (RJASR), que lista as circunstâncias da utilização de informações confidenciais.

Para além do RJASR, o Regime Jurídico do Contrato de Seguro, (doravante denominado por RJCS) aprovado pelo Decreto-Lei nº 72/2008, de 16 de abril[16], alterado pela Lei nº 147/2015, consolida "num único diploma, o regime geral do contrato de seguro, evitando a dispersão e fragmentação legislativa e facilitando o melhor conhecimento do regime jurídico por parte dos operadores". Integra também uma disposição que estabelece um nexo entre o regime jurídico da atividade seguradora e as normas contratuais.

A reforma do RJCS assenta primordialmente numa adaptação das regras em vigor, procedendo à atualização e encadeamento de conceitos de diversos diplomas, preenchendo certas lacunas. Regula alguns casos omissos na atual legislação e introduz diversas soluções normativas inovadoras. Importa referir que a consolidação e adaptação do regime do contrato de seguro tem especialmente em conta as soluções estabelecidas no direito comunitário, já transpostas para o direito nacional, com especial relevo para a proteção do tomador do seguro e do segurado[17], nos designados seguros de riscos em massa.

Alavancando a continuidade do raciocínio, as leis em matéria de seguros impõem às seguradoras a obrigação de elaborar e entregar ao contratante do seguro uma política que declare os direitos e obrigações das partes (entre outras condições), o que é denominado por apólice. As apólices são específicas para cada tipo de atividade (González, 2017). A apólice de seguro está para o segurado e seguradora, assim como a lei está para o cidadão e para o Estado, ou seja, a apólice (ou contrato seguro) acaba por ser a lei pela qual se rege toda a atividade e base de contratação de um seguro. Contudo a apólice é já um documento particular e que depende de caso para caso, pelo que sendo fruto do produto que se pretende contratar, não se entrará aqui em detalhe, sendo apenas de breve menção a parte legal da mesma (Van Houtte, 1994).

[16] Pelo conferido a nível do preâmbulo deste Decreto-Lei, sabe-se que "o seguro tem larga tradição na ordem jurídica portuguesa. No entanto, a legislação que estabelece o RJCS encontra-se relativamente desatualizada e, à mercê de diversas intervenções legislativas em diferentes momentos históricos, pelo que nem sempre há harmonia de soluções".

[17] Prescreve-se a designada imperatividade mínima com o sentido de que a solução legal só pode ser alterada em sentido mais favorável ao tomador do seguro, ao segurado ou ao beneficiário. Também em termos de nulidade do contrato seguro a mesma não opera em termos desvantajosos para o tomador.

Com a realização de um contrato seguro, instrumentaliza-se um negócio jurídico com fim económico-social e interesses legítimos baseados na boa fé e confiança que inspiram uma relação jurídica[18]. Todos estes objetivos, de acordo com as pretensões determinadas pelas partes, geram um vínculo e efeitos jurídicos tutelados pelo ordenamento jurídico aplicável (Fraguio & Macías, 2011).

A proposta de seguro, que surge enquanto simulação da apólice a ser celebrada, deve conter uma menção comprovativa de que as informações que o segurador tem de prestar foram dadas a conhecer ao tomador do seguro antes de este se vincular, (art.º 21º, nº5 do RJCS). Ao segurador cabe o dever especial de esclarecimento previsto no art.º 22º do RJCS, devendo o mesmo antes da celebração do contrato, esclarecer o tomador do seguro acerca de que modalidades de seguro, entre as que ofereça, são convenientes para a concreta cobertura pretendida. Tal incumbência, também é válida para chamar atenção sobre exclusões da apólice, o que raramente é feito pela parte comercial (mediação de seguros e corretoras).

No capítulo II, parte especial, e subsecções sequentes do RJCS, abordam-se vários tipos de seguros existentes (incêndio, financeiro, pecuário, de vida, de saúde), sendo que não está contemplado, nem tão pouco previsto, a tipologia de seguro informático, ou associado, quer a tecnologias de informação e comunicação – doravante denominadas de TIC- quer a sistemas tecnológicos e redes. O seguro informático pode ser considerado como um seguro misto, por conta própria e por conta de outrem, já que tanto é válido para proteção da esfera própria como de terceiros – informações/dados de outrem[19].

[18] O RJCS distingue os vários planos jurídicos de relevância, no que respeita ao contrato seguro como as menções que devem constar obrigatoriamente na apólice e certas cláusulas, designadamente as que excluem ou limitam a cobertura, têm de ser incluídas em destaque, de modo a serem facilmente detetadas.

[19] Importa esclarecer, a título exemplificativo, que um seguro informático pode ser contratado com especial enfoque para a proteção própria de uma empresa, seja em termos de ativos, dados, fórmulas, e propriedade digital na rede (e que poderão resultar em perdas de informação críticas para o próprio segurado), ou, para salvaguarda de danos a clientes ou outros parceiros de negócios, no caso de informações em comum serem comprometidas (e aí poderão resultar danos na ordem da responsabilidade civil, com prejuízos para outrem). Usualmente, apólices contemplam verbas próprias contando também com capitais específicos para RC, o que o torna um seguro misto.

No que respeita à natureza jurídica de alguns contratos, sobretudo contratos de seguro no âmbito informático, este acaba por ser um contrato atípico que carece de regulação própria e não está regido por uma normativa legal especial. É um contrato complexo[20] que surge de diversos vínculos jurídicos, e não depende de outro contrato que lhe seja precedente (González, 2017). Esta peculiaridade do contrato informático, destaca-se na desigualdade[21] existente entre as partes contratantes, tanto num plano técnico como económico. O provedor (seguradora) ostenta uma posição financeira mais forte que a empresa (cliente), e, os conhecimentos técnicos terão de ser equilibrados com os do cliente, contando com profissionais com capacidade técnica adequada e competente (Arien, 2003).

Nesta senda, resume-se sempre à aceitação, ou não, das condições gerais e particulares que o cliente analisará, e que raramente são modificadas ou negociadas. Baseando-nos no princípio da boa-fé, a que presidem os vários contratos, tal como estabelece o art.º 3º do Código Civil, a obrigação da informação, aconselhamento e assessoria por parte do contratante mais informado, seja o provedor ou cliente, adquire uma importância decisiva no âmbito contratual informático. As obrigações não consistem apenas em informar em sentido estrito, mas sim indicar-se a solução mais vantajosa e moldável às necessidades da parte contratada, passando pela aplicação de *frameworks* como a que se propõe, para uma correta análise de risco, e conhecimento ambivalente dos factos à data de início da apólice (Arien, 2003).

Assim, não poderíamos deixar de ressalvar que, em primeira instância, estão os diplomas gerais, tais como o Código Civil, e, se este falhar, em face da danosidade social consequente, entrará o Código Penal (designado, adiante, por CP), e só posteriormente a apólice de seguro em si. Contudo, invertendo o funil da perceção, a

[20] Segundo o art.º 5º do RJSC, ao contrato de seguro aplicam-se as normas gerais de direito internacional privado em matéria de obrigações contratuais, nomeadamente as decorrentes de convenções internacionais e de atos comunitários que vinculem o Estado Português. Pelo princípio geral elencado no art.º 11º do RJCS, o contrato de seguro rege-se pelo princípio da liberdade contratual, tendo carácter supletivo as regras constantes do presente regime, com os limites indicados na presente secção e os decorrentes da lei geral.

[21] A desigualdade entre as partes leva à conclusão de que o objeto da contratação, neste caso dados, ativos, informações confidenciais, devem ser especificados com terminologia e detalhe perfeitamente compreensíveis e transparentes. Este tipo de seguro, deve ser redigido de forma especialmente minuciosa (Arien, 2003).

apólice de seguro será sempre a primeira base de interpretação utilizada para compreender qualquer sinistro ou litígio, dado que na mesma vêm especificados o clausulado contratado, capitais e verbas discriminadas, que devem ser do conhecimento total do segurado. O âmbito da atuação da vontade das partes (cliente e seguradora) é amplo, embora se levante sempre a necessidade de adaptação a tipos legais já existentes (Arien, 2003).

Em caso de discordância quanto às causas do sinistro, esse apuramento pode ser entregue a peritos árbitros nomeados pelas partes, nos termos previstos no contrato ou convenções anteriores, para peritagem e contra peritagem (art.º 50º do RJCS).
Nestes casos, por eventual desacordo, não aceitação das conclusões do processo de averiguação de sinistro ou oposição ao apuramento das peritagens, enquanto nota intercalar e sem mencionar detalhes da Lei nº 63/2011, de 14 de dezembro[22], da Lei nº 29/2013, de 19 de abril[23] , da Lei nº 14472015, de 8 de setembro[24] ou do DL nº94B/98 de 17 de abril[25], importa referir que existem várias normas e circulares que regulam práticas, apólices e deveres legais dos seguradores e entidades do ramo.

Este tipo de processos[26], aquando de um não acordo, são resolvidos, em primeira instância, e na esmagadora maioria dos casos, em Julgados de Paz[27], ou nos Centros

[22] Lei da Arbitragem Voluntária.
[23] Lei da Mediação.
[24]Estabelece o enquadramento jurídico dos mecanismos de resolução extrajudicial de litígios de consumo.
[25] Regula as condições de acesso e de exercício da atividade seguradora e resseguradora no território da Comunidade Europeia.
[26] O Capítulo I e II do anexo II da Lei nº147/2015 de 9 de setembro, que aprova o RJASR, prevê os ilícitos penais e aspetos associados, desde aquisição da notícia do crime, averiguações preliminares, medidas cautelares, segredo de justiça, acusação e defesa, entre outras diretrizes para casos que fujam à regular normalidade do processo de sinistro ou seguro, tal como posteriores impugnações judiciais, (secção II).
[27] Os Julgados de Paz são tribunais dotados de características de funcionamento e organização próprias, que se encontram em funcionamento desde 2002. A base legal que deu suporte à sua criação foi a Lei n.º 78/2001, de 13 de julho - Lei de Organização, Competência e Funcionamento dos Julgados de Paz, comumente denominada Lei dos Julgados de Paz - a qual foi pela primeira vez alterada pela Lei n.º 54/2013, de 31 de julho. Os Julgados de Paz são competentes para resolver causas comuns de natureza cível, cujo valor não exceda os €15.000 (excluindo as que envolvam matérias de Direito da Família, Direito das Sucessões e Direito do Trabalho), e assentam, numa parceria pública entre o Ministério da Justiça e as autarquias (Fonte: Retirado de Direção Geral da Política de Justiça, em https://www.dgpj.mj.pt/).

de Informação, Mediação, Provedoria e Arbitragem de Seguros (CIMPAS) [28]. Também se deverá, em casos de fraudes, recorrer a instâncias judiciais.

Relativamente ao CP, este tipifica como crime determinados comportamentos, lesivos, resultantes do exercício da atividade seguradora, no capítulo que aborda os crimes contra o património, nomeadamente no art.º 219º, este prevê e pune a burla relativa a seguros, com pena de prisão (entre três anos a oito anos, consoante as circunstâncias do crime) ou com pena de multa. É um crime cujo procedimento criminal depende de queixa, de natureza semi-pública, sendo a tentativa punível.

No caso de quem receber ou fizer com que outra pessoa receba valor total ou parcialmente seguro, seja provocando ou agravando um resultado, ou causando a si próprio lesão cujo risco está coberto, será igualmente punido (art.º 219º, nº1). Se o prejuízo patrimonial provocado for de valor elevado, a moldura penal é, naturalmente, agravada.

Por isto, e enquanto únicas menções constantes no CP relativa a matéria de seguros, este mostra uma preocupação superficial do legislador com lesões que possam defraudar uma seguradora, pelo que a doutrina não tem desenvolvido avanços significativos em matéria de situações fraudulentas contra entidades seguradoras.

Importa, por último, realçar o DL nº 28/84, de 20 de janeiro, sobre as Infrações Antieconómicas e Contra a Saúde Pública, onde, no seu artº. 36º se prevê a fraude na obtenção de subsídio ou subvenção (com definição no seu artº. 21º)[29], sendo que a fraude a entidades seguradoras se poderá enquadrar também neste regime. Foram também superficialmente analisados outros regulamentos que, sendo laterais ao tema, se encontram resumidos, de forma breve, na tabela V constante em apêndice (ponto 9.1) sendo que a Lei do Cibercrime será mencionada seguidamente.

[28] O CIMPAS é uma entidade apoiada e autorizada pelo Ministério da Justiça, que tem por objeto prestar informações e disponibilizar vias de resolução através de procedimentos de mediação e da arbitragem (Fonte: Retirado de https://www.cimpas.pt/pt).

[29] O bem jurídico tutelado pela norma que prevê e pune o crime de fraude na obtenção de subsídio ou subvenção reside, por um lado, na confiança na vida económica, e, por outro lado, na correta aplicação dos dinheiros públicos no domínio da economia.

3.2. Crimes Informáticos, Lei do Cibercrime e outros diplomas legais

Da mesma forma que, um seguro informático prevê riscos informáticos, e ainda infrações conexas com o cibercrime, é perfeitamente conveniente enquadrar os mesmos perante uma ótica jurídica.

É possível dizer que, tanto do ponto de vista jurídico como do setor segurador perante um sinistro do género, existe uma bipolarização acerca do objeto dos crimes informáticos, em que, por um lado temos a proteção dos sistemas, e por outro, temos a corrente que pugna pela proteção dos dados e das informações encerradas no sistema informático (Neto, 2003) e (Santos, 2017).

Em consonância com os desenvolvimentos positivos da "era digital", a sociedade atual vê-se também com graves problemas em mãos, face à metamorfose das interconexões virtuais, e é no âmbito do direito que essas dificuldades são mais compreensíveis. Não só pelo facto de os crimes reais serem cometidos através de um computador, Internet ou outro dispositivo com as mesmas capacidades, como também devido ao facto de o próprio equipamento ser o alvo da penetração ilegítima, constituindo-se como um desafio para o legislador e para a jurisprudência[30]. As ações repressivas são de extrema dificuldade de controlo, dadas as diferenciações, quase sempre verificadas, entre o país alvo do ataque e o país da sua autoria, com distintas jurisdições (Verdelho, 2003) e (Santos, 2015).

Apesar das dificuldades, desde 2002 que têm havido avanços importantes no sentido de incluir figuras penais que tornem puníveis ilícitos informáticos, seja sobre infrações informáticas, contra a informação protegida, destruição maliciosa de documentos, falsificação eletrónica, danos informáticos[31], como também sobre

[30] Isto significa que a identificação de um equipamento através do qual se cometeu um determinado crime, não é a mesma coisa que determinar o suspeito que está por detrás de tal operação, dado que as penas e medidas a aplicar pela lei serão direcionadas ao operador e não à máquina em si. A determinação atempada e concreta de um criminoso que comanda a máquina, e o estabelecimento do nexo causal entre a sua ação e a concretização de um crime, será sempre um desafio para os investigadores criminais e juristas.

[31] "Quem, maliciosamente, de qualquer forma ou use qualquer método, destrua, altere, desative, exclua ou provoque danos, temporariamente ou permanentemente, os programas, dados, bancos de dados, informações

divulgação ou utilização fraudulenta de informação protegida, destruição de instalações para transmissão de dados, apropriação ilícita, entre outros. Contudo, importa mencionar que dos poucos diplomas existentes, os mesmos não são suficientes para cobrir este fenómeno nem tão pouco esclarecê-lo na íntegra, pois não abordam adequadamente as questões mais complexas. (Fitzpatrick & Dilullo, 2015).

Assim, torna-se necessário uma transformação das medidas a tomar para combater estes crimes que fogem do tradicional horizonte jurídico, o que obrigará a uma mudança de paradigma, que será difícil de alterar. Existem algumas dificuldades que se registam não só na investigação de crimes em ambiente digital (resultantes de um conjunto de vários fatores, como por exemplo a não precisão da localização física dos agentes, a imaterialidade associada e também a (in) determinação de jurisdição), como também pela impunidade deste tipo de ilícitos, pois nem todos se adequam ao tipo previsto nos tradicionais crimes do CP nem na Lei do Cibercrime (doravante denominada por LC)[32]. Contudo, alguns esforços e medidas têm sido tomados nesse sentido, como a criação da UNC3T[33] e do CNCS[34], (Dias, 2012), (Gómez e Espinosa, 2014) e Azevedo, 2016).

Segundo Cazelatto & Moreno (2016), o cibercrime é um problema que é preciso encarar através de várias facetas, a de gestão, a organizativa, a técnica, a tecnológica e a legal. De acordo com esta última, a dimensão informática trouxe conflitos à ordem jurídica, tendo os juristas vindo a fazer esforços no sentido de tutelar o espaço virtual, com muralhas digitais que se constituem como obstáculos relativamente à regulamentação da rede. Estamos perante um novo paradigma social e jurídico, em

ou qualquer mensagem de dados contida num sistema de informação ou rede eletrónica, será punido com prisão de 6 meses a 1 ano, e coimas" (Gómez e Espinosa, 2014)

[32] Aprovada pela Lei nº 109/2009 de 15 de setembro, que transpõe também para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

[33] A Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica, que goza de autonomia técnica e científica, apoia investigações, assegura o ponto de contacto operacional, e principalmente tem competências de prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias relativamente aos crimes previstos na LC, entre outras (Fonte: https://www.policiajudiciaria.pt/unc3t/).

[34] Centro Nacional de Cibersegurança, criado em 2012, o qual faz análise e prevenção de ataques, mas não a monitorização de todos os organismos públicos. Constitui a primeira linha de defesa dos serviços públicos a ataques informáticos (Fonte: https://www.cncs.gov.pt/)

que a mudança de hábitos alavanca por sua vez uma mudança de postura jurídica, para que o direito acompanhe as necessidades humanas (Bacelar, 2017) e (Pereira, 2017 a).

Destarte, o enquadramento jurídico do cibercrime é difícil de solucionar, pois as leis são tradicionalmente criadas para a proteção de objetos materiais e não de objetos imateriais, como as informações, movimentos *online* e dados guardados em suporte digital. Contudo, existem opiniões distintas, e em alguns casos defende-se que, este tipo de criminalidade pode ser combatida analogamente com os instrumentos penais tradicionais, e, noutros, que é necessária a adoção de novos instrumentos penais tecnológicos. De facto, a ausência de legislação criada para acautelar a utilização da tecnologia constituirá uma lacuna, na medida em que na falta ou omissão de menção na lei, será sempre o acusado/suspeito, ilibado (Bacelar, 2017).

Isto deixa uma vasta gama de condutas ilícitas em dúvida quanto à sua tipificação e/ou punição, pois é sem sombra de dúvidas, um sistema ágil e em expansão, como hoje tão facilmente vemos sob a forma de pessoas a trabalhar a partir de casa, negócios fundados com base em *networking* e cadeias de *start-ups*, com propostas aliciantes de liberdade financeira (Neto, 2003) e (Santos, 2015).

Não sendo possível aqui explorar exaustivamente todo o referido quadro legal, não podemos deixar de fazer menção a algumas das disposições da lei fundamental, a Constituição da República Portuguesa (adiante denominada por CRP). A CRP no seu art.º 35º, nº6 determina que "A todos é garantido livre acesso às redes informáticas de uso público (…)", e no art.º 37.º estabelece a liberdade de expressão e informação, e concretiza na sua redação que todos têm o direito de exprimir e divulgar livremente o seu pensamento, por qualquer meio, sem impedimentos nem discriminações. Sabendo nós que, como regra, as normas legais não podem prevalecer sobre os princípios fundamentais do Estado de Direito Democrático protegidos pela CRP, facilmente entendemos a dicotomia segurança/liberdade e a necessidade de balançar estes valores, quando falamos em governação da Internet (Veiga & Dias, 2010) e (Bacelar, 2018).

Este "mundo em rede" desenvolveu um novo plano de condução de conflitos com características únicas, que obriga a uma redefinição das políticas de segurança/ defesa nacionais. Devem ser prevenidos crimes, identificados e condenados os responsáveis, atuando segundo as regras do sistema judicial e dentro do quadro da legislação aplicável, cujos autores serão naturalmente o Ministério Público (adiante MP), os Órgãos de Polícia Criminal (adiante OPC's) e Magistrados Judiciais (Bravo, *et al* 2012).

Segundo Veiga e Dias (2010), domina-se hoje a governação mínima que concilie a liberdade com a necessária privacidade, segurança e respeito pelos direitos, liberdades e garantias de cada um, e de terceiros. A CRP é mecanismo regulador de toda a ordem política e jurídica do Estado, pelo que a informação é um bem jurídico que merece toda a atenção face à globalização operada por meios informáticos. Contudo, todos temos direito à informação, e todas as comunicações devem ser tratadas de forma igual, qualquer que seja a informação, o destinatário, ou a fonte, sob o fundamento de que a Internet não deve conter restrições políticas nem técnicas. Apela-se aqui ao princípio da neutralidade da rede[35], da privacidade do usuário e da liberdade de expressão, os quais devem ser explorados através da ponderação dos princípios constitucionais da proporcionalidade e da razoabilidade (Pereira, 2017 a).

Desta forma, entende-se que, grande parte da criminalidade informática tem visado ataques a bens jurídicos já tradicionalmente protegidos pelo ordenamento penal (saúde, segurança, bem-estar, liberdade). Contudo, a nova delinquência recai sobre os próprios elementos constituintes da informática (a máquina e os seus componentes) bem como sobre programas, *hardware*, dados ou documentos em formato eletrónico.

Assim, a informação constitui-se como o principal bem jurídico, e complementarmente também os sistemas e dados, pois estes últimos são os mecanismos materiais, por onde se desenrola o armazenamento, tratamento e

[35] A rede não é neutra – contraria o princípio da neutralidade da rede (é um espaço livre de interferência, onde os cidadãos expressam os seus argumentos de forma igual) (Santos & Guedes, 2015).

transferência. Contudo, nem sempre é fácil definir o bem jurídico afetado, o que deturpa um pouco a forma como o direito atua nestes casos, os mecanismos de aplicação da lei, e as naturais questões éticas que, em paralelo, se colocam (Lima, 2017) e (Bacelar, 2018).

Ainda nesta aceção, há quem defenda a aplicação de penas mais severas concernentes a estes crimes, pois acredita-se que as punições previstas na legislação vigente não são proporcionais ao impacto e prejuízo que a usurpação da Internet podem causar a uma pessoa e/ou empresa (Molitor & Velazquez, 2017). Exemplo disso é a burla informática, prevista no art.º 221º CP, a devassa por meio de informática (art.º 193º CP) e a violação de correspondência ou de telecomunicações (art.º 194º CP). Os mecanismos conducentes ao cometimento de alguns destes tipos criminais levam a que se reúnam elucidações que coadjuvam na consciencialização de magistrados e juristas, e que serão favoráveis à melhor compreensão e aplicação do direito, na justiça e tribunais.

Para além do CP que como já se referiu, fixa, especialmente, o regime jurídico da burla informática, entre outros ilícitos que se interrelacionam com a cibercriminalidade, é a LC que se destaca enquanto diploma fundamental na classificação das principais condutas criminais em termos informáticos. Esta nova lei, pretende uma harmonização das legislações nacionais dos EM da UE em matéria de criminalidade cometida por estes meios, bem como facilitar a cooperação internacional e as investigações de natureza criminal. Tipifica cinco crimes informáticos em sentido estrito: a falsidade informática (art.º 3.º), o dano relativo a programas ou outros dados informáticos (art.º 4.º), a sabotagem informática (art.º 5.º), o acesso ilegítimo (art.º 6.º), a interceção ilegítima (art.º 7.º) e a reprodução ilegítima de programa protegido (art.º 8.º).

Mais ainda, prevê-se na LC a preservação e revelação expedita de dados informáticos para efeitos de investigação criminal, fixando-se prazos rigorosos para a salvaguarda dos mesmos (por exemplo, o RGPD prevê já coimas aplicáveis quando estes prazos não são cumpridos). Neste campo, a cooperação vai assim para além dos operadores

da justiça, abrangendo os prestadores de serviços de comunicações eletrónicas. Trata-se, portanto, de uma lei aplicável aos riscos (e crimes informáticos), cometidos por via eletrónica e, ainda aos ilícitos cuja prova esteja guardada em suporte digital (Veiga & Dias, 2010).

3.3. Breve perspetiva da fraude ao seguro e matéria de risco

A fraude aos seguros[36] é um fenómeno que se verifica no mundo inteiro e, apesar de alguns países serem mais eficazes no combate a estas práticas do que outros, não deixa de ser um problema relevante e extremamente atual. "Praticar fraude seja em que ramo de sinistro, é crime, e traz impactos significativos e diretos para os resultados das seguradoras, para o segurado honesto e para a sociedade em geral. Também o aumento de ocorrências fraudulentas acarreta a elevação de custos de peritagem, pagamentos e consequentemente aumentará os prémios de seguros" (Pereira, 2013). Tudo isto é diretamente transposto para a ordem jurídica na medida em que a fraude é transversal a todos os ramos de seguros, não apenas aos seguros informáticos.

Na esmagadora maioria dos casos (processos de regulação de sinistros) em que a seguradora não tem provas fidedignas e sólidas para lutar contra a fraude e defender a sua posição em Tribunal, a mesma não irá contra o segurado, pelo contrário tenta muitas vezes chegar a um acordo com o mesmo, por menores valores face aos reclamados. Caso o fizesse, só iria denegrir a sua imagem social.

Este tipo de situações começa a surgir com maior frequência, pelo que é cada vez mais necessário, seja em volta da seguradora (em principal) mas também nas

[36] Sobre a gestão de riscos e comunicação de situações fraudulentas, tem-se o previsto no art.º 13º do RJASR – "As empresas de seguros e de resseguros devem (…), definir uma política de prevenção, deteção e reporte de situações de fraude nos seguros, estabelecendo a ASF -APS, por norma regulamentar, os princípios gerais a respeitar no cumprimento deste dever". Ainda se acrescenta que o modelo de fraude e ataques informáticos acomodaram-se na rede com uma infinidade de técnicas distintas e polivalentes. Assim, neste ambiente, as manifestações fraudulentas são peculiares e muitas delas não conseguem ser processadas do ponto de vista jurídico. A escassa adaptação do meio ambiente, as circunstâncias em que manobram os criminosos, bem como a perceção limitada do risco, contribuíram para o impulsionamento do fenómeno (Teruelo, 2007).

entidades particulares (em que se apoia e delega serviço de peritagem e averiguação), a criação de medidas de deteção e controlo de fraudes. Ao ser perpetrada uma fraude, é violado o princípio da boa-fé, que acompanha a celebração de um contrato seguro, onde deveria sempre prevalecer a honestidade das partes. A maioria das seguradoras considera que os comportamentos fraudulentos são próprios dos anos recentes, não constituindo propriamente uma novidade neste mercado (Gómez e Espinosa, 2014).

A fraude é considerada um mal crónico sofrido pelo mercado segurador, com consequências que vão além do prejuízo das companhias. Ainda que minoritários, há registos de casos que prevalecem em tribunal, e consegue-se provar a índole criminal associada, embora regra geral, acabe no pagamento de uma multa por parte do segurado, e não numa real condenação. A fraude aos seguros constitui um crime punível por lei (art.º 219º CP), mas em todo o desenrolar do processo, tem um tratamento bastante delicado. Os riscos de fraude, podem produzir-se tanto por referência à declaração de sinistro, como à subscrição de apólices com intenção de enriquecimento injusto, alheio à própria essência do objeto do contrato seguro (Pazmiño *et al* ,2017).

No que respeita a matéria do risco, de particular relevo no contrato de seguro, surge regulada, primeiro, em sede de formação do contrato, seguidamente, na matéria do conteúdo contratual e, de seguida, a propósito das vicissitudes, mantendo sempre um vetor: o risco é um elemento essencial do contrato, cuja base tem de ser transmitida ao segurador pelo tomador do seguro, atendendo às diretrizes por aquele definidas. Também no caso do risco se alterar, deve ser sempre comunicado ao segurador, em virtude de poder diminuir ou agravar o risco. Nesta senda, o art.º 24º do RJCS remete para que uma qualquer empresa que venha a fazer um seguro, tenha de ser transparente ao fornecer os dados que dispõe e partilhar a veracidade da realidade interna à organização[37].

[37] "O tomador do seguro ou o segurado está obrigado, antes da celebração do contrato, a declarar com exatidão todas as circunstâncias que conheça e razoavelmente deva ter por significativas para a apreciação do risco pelo segurador." (art. 24 º, nº1 do RJCS);

Concernente à declaração inicial de risco, foram reduzidas as incertezas das soluções jurídicas, mantendo-se a regra que dá preponderância ao dever de declaração do tomador sobre o ónus de inquérito do segurador, onde são introduzidas exigências a este último, nomeadamente impondo-se o dever de informação ao tomador do seguro sobre o regime relativo ao incumprimento da declaração de risco. Haverá também a distinção entre comportamento negligente ou doloso do tomador de seguro, com consequências diversas quanto à validade do contrato[38]. Esta disposição é de especial importância no âmbito dos seguros informáticos, dado que nem sempre é simples uma quantificação ou caracterização do risco, e, também, uma omissão sobre algum conteúdo ou detalhe técnico, pode ser considerado bastante grave e ter repercussões amplamente nefastas numa situação de sinistro (ponto V do preâmbulo do RJCS).

Assim, há que ter em conta que, não se indemnizam danos derivados de qualquer risco, pois a insegurança pode ser técnica ou jurídica. De uma ótica jurídica, a expressão do risco tem como referência as vicissitudes fortuitas, não imputáveis a dolo ou negligência do sujeito concreto, a respeito dos quais se devem decidir o regime de riscos que padecem os bens em sentido jurídico. Há consequências jurídicas que se produzem em virtude da realização do risco. Já da ótica técnica, respeita ao sistema de segurança e política de defesa do cliente/empresa, que deveriam ser acautelados a todo o minuto (Fraguio & Macías, 2011) e (Pereira, 2017).

É, pelo exposto, percetível a existência de vários riscos associados à atividade, de ambas as frentes (segurado e segurador) com implicâncias tanto a nível de possíveis fraudes, como de violações do princípio de boa fé da relação comercial. Destarte, é conveniente proporcionar às empresas de seguros e de resseguros um enquadramento legal para o exercício da atividade em todo o mercado interno, facilitando a estas empresas, a cobertura de riscos e compromissos nela situados. Desta forma, em consonância com a evolução mais recente em matéria de gestão de riscos, é crucial adotar uma abordagem económica baseada no risco, incentivando, assim, as empresas

[38] "O segurador e segurado devem comunicar reciprocamente as alterações do risco respeitantes ao objeto das informações (…)" (art. 91º nº 1); "o tomador do seguro tem o dever de dar conhecimento do facto, comunicar ao segurador todas as circunstâncias que agravem o risco (art. 93º nº1) RJCS.

a avaliarem e gerirem corretamente os seus riscos, segundo um nível de harmonização[39] (Gomes, 2017).

Sendo a revolução tecnológica uma grande oportunidade transversal para o sector financeiro, no domínio segurador (e outros), esta comporta riscos que devem ser avaliados juridicamente, e também regulados em certos casos. Este tema da *FinTech*[40] está presente em diversas iniciativas legislativas e políticas de natureza geral ou estrutural, como por exemplo no RGPD, que introduz novas figuras impostas pela tecnologia, como decisões automatizadas, direito a portabilidade de dados, formulação de perfis, entre outros. Temos vindo a observar uma mudança de atitudes por parte dos utilizadores destes serviços, com uma digitalização dos serviços financeiros, entrada de novos intervenientes, etc (Cordeiro, et al 2017).

São identificados desde riscos contratuais[41] a riscos legais/jurídicos[42], para além dos já mencionados, o que também se prende com os riscos comerciais afetos, na medida em que as companhias de seguros, e outras instituições, deparam-se com a necessidade de adotar novos canais de comercialização dos seus serviços e novas formas de apresentar os seus produtos. Pode resultar um risco relevante para as pequenas e médias seguradoras, pelo que estas têm de dispor de mais recursos para uma melhor capacidade de adaptação entre as alterações internas (à atividade seguradora) e externas (em matéria jurídica e jurisprudencial).

Deve, assim, haver uma modernização dos contratos já existentes (aqui inserem-se taxativamente os seguros informáticos), pelo que deve ser tido em atenção os comportamentos e tendências das diferentes faixas etárias da população, diferentes

[39] Conforme explanado na Diretiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, relativa à atividade e exercício de seguros e resseguros.
[40] *FinTech* reporta a junção de Finanças e Tecnologia. A Comissão Europeia define como sendo inovações tecnológicas com implicações potencialmente transformadoras para o sistema financeiro, para os seus intermediários e utilizadores (Fraguio & Macías, 2011)
[41] Derivados de erros de interpretação de clausulado, deficiências na redação dos contratos seguros e apólices subscritas, riscos motivados por possíveis efeitos do instrumento contratual, relações jurídicas derivadas do mesmo e o (in)cumprimento dos compromissos bilaterais adquiridos, cláusulas limitativas, omissas, abusivas/lesivas, supressivas etc (Fraguio & Macías, 2011).
[42] Derivados do incumprimento das normais legais em vigor, ou incumprimento de obrigações jurídicas adquiridas em virtude do contrato seguro realizado com a outra parte, bem como da incorreta interpretação e aplicação da legislação vigente (Fraguio & Macías, 2011).

linhas empresariais e sectores de negócio. No âmbito da experiência digital e diferentes segmentos de consumidores, temos por um lado a Geração X (utilizadores recorrentes de ferramentas mecânicas, que recorrem pontualmente à tecnologia) a Geração Y (*Millenials*) e a Geração Z (*Digital Natives*), estes últimos dois, consumidores vorazes de tecnologia (Fraguio & Macías, 2011).

Isto implica que o mercado segurador tenha de estar em constante análise das tendências e expectativas dos clientes, em paralelo com um modelo de negócio ágil e uma integração tecnológica, para proporcionar aos segurados o que desejam e de encontro com às expectativas da procura. Se isto não ocorrer, e não se adaptarem a novos modelos de seguros, pode haver uma quebra de relação e confiança, dado que estas gerações - Y e Z - facilmente, e cada vez com maior frequência, mudam de instituição, recorrendo a outras seguradoras fora do mercado nacional (Cordeiro et al, 2017).

3.4. Na ótica do Direito Virtual – enquadramento legal em matéria de cooperação internacional

O Direito pode ser entendido como uma "tecnologia social de prevenção e controlo de riscos", garantindo a segurança, na Internet. Na UE, o Direito procura ter respostas para os riscos tecnológicos, mesmo que generalizados, atendendo ao novo paradigma explicativo da sociedade do risco. Nesta sociedade, o risco é generalizado, as ameaças apesar de naturais na sua aparência, são essencialmente tecnológicas, e a perceção social do risco e insegurança passam a ser permanentes (Masseno, 2011) e (Bacelar, 2017).

A Lei de Política Criminal referente ao Biénio 2017-2019[43], na continuidade das anteriores, estabelece e elenca crimes de carácter prioritário, seja em termos de prevenção como de investigação, já que a insuficiente cooperação internacional no

[43] Que define os objetivos, prioridades e orientações de política criminal para o biénio de 2017 -2019.

âmbito dos crimes informáticos pode pôr em causa a eficácia do exercício da ação penal (Veiga, & Dias, 2010). Segundo o art.º 2º al. c) desta mesma lei sabe-se que o cibercrime é considerado um fenómeno criminal de prevenção prioritária, cuja competência legal de prevenção e investigação criminal, está atribuída à PJ.[44] De acordo com Bernal, (2009) "o desafio é saber até que ponto a regulação existente, que ainda não está harmonizada[45], e as práticas atuais dos reguladores, são adequadas, e, em que aspetos deverão ser alteradas, face às novas realidades emergentes".

A LC[46] concretiza aquilo a que Portugal se obrigou no âmbito da Convenção sobre o Cibercrime[47], sendo estes instrumentos de cooperação internacional de grande relevo, na luta contra a criminalidade informática (Veiga & Dias, 2010). Segundo o art.º 20 da LC, as autoridades nacionais competentes cooperam com as autoridades estrangeiras habilitadas para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico, de um crime. Também prevê genericamente, embora com mais desenvolvimentos, os termos da cooperação internacional, entre os arts.º 21º e 26º da presente lei (Masseno,2011a).

Esta Convenção é uma referência de fundo que, recorda os princípios da legalidade e da territorialidade[48] em matéria penal, a necessidade, absoluta, de pontos de referência normativos acima dos Estados soberanos e de cooperação entre as polícias e autoridades judiciais dos diversos Estados. Pretende uma harmonização de

[44] Cf. art.º 1º e art. 7º, nº3 al. l) da LOIC, e, arts.º 4º e 5º da LOPJ - Lei n.º 37/2008 de 6 de agosto.

[45] Algumas jurisdições estão a pôr em prática legislação nacional para enquadrar algumas atividades relacionadas às *FinTech*, pela ausência de um modelo regulatório harmonizado. Isto poderá gerar modelos de supervisão distintos entre os vários países, e criar distorções a nível transfronteiriço e regulatório (Cordeiro, *et al* 2017).) Tudo isto requer uma mudança fundamental na atuação do Direito, e, as medidas legislativas adotadas pela UE devem ser realizadas, tal como uma consciencialização global no sentido da literacia informática a todos os níveis (Santos, 2015).

[46] O CP não engloba diretamente crimes de índole informática, os quais se encontram expressos na LC.

[47] Também denominada de Convenção de Budapeste, que impôs a modificação do direito interno dos Estados signatários, dando origem em Portugal à LC em setembro de 2009. Esta convenção constitui-se como o primeiro tratado internacional que dispõe sobre os crimes cometidos através da rede mundial de computadores, procurando abordar a cibercriminalidade e harmonizar as legislações nacionais, melhorar técnicas e aumentar a cooperação entre as nações.

[48] A problemática da competência territorial, a natureza multi-jurisdicional da Internet, a qualificação do crime ou moldura penal e a dificuldade na determinação do local onde o crime foi perpetrado, constituem-se como obstáculos no entendimento e tratamento deste tipo de criminalidade (Azevedo, 2016**).**

legislações e do próprio direito penal material, atendendo às peculiaridades destes crimes, tendo como conteúdos o direito penal substantivo (art.º 2º a 13º), o direito processual penal (art.º 14º a 22º) e a cooperação internacional (arts.º 23º a 35º).

Desta forma, Portugal tem um quadro jurídico atualizado que se baseia, como já foi suprarreferido, na Convenção de Budapeste e na LC. Também transpôs os instrumentos legais da UE mais relevantes, como as decisões quadro no combate a ataques contra sistemas de informações (Dec. 2005/22/JHA) de 24 de fevereiro de 2005) (Masseno, 2015).

Fruto das insurgentes notícias acerca de infortúnios informáticos e intrusões indesejadas nos serviços, empresas e demais, há uma crescente atenção para os problemas na área da governação da Internet, e a Europa será naturalmente, uma das regiões do globo onde há uma maior estruturação do pensamento nesta área. Foi assim criado um fórum de discussão destes temas, o EuroDIG, onde se estudam e discutem os desafios presentes e futuros que a Internet está a trazer para a agenda da sociedade europeia[49]. Também existem a nível da UE instituições que combatem diariamente as ameaças colocadas por este fenómeno criminal, entre as quais destacamos a Europol[50], EC3 e a AED, constituindo três agências ativas no campo da repressão/defesa, com conselhos de administração em que estão representados os EM e que se constituem como plataformas de coordenação a nível da UE (Verdelho, 2003).

3.5.Regulamento Geral Sobre a Proteção de Dados

Quando se fala dos aspetos legais da Internet, surgem algumas pedras de toque que necessariamente se abordam em discussões jurídicas como é o caso da proteção de

[49] Uma das metas da Estratégia Europa 2020 trata-se da promoção da sociedade digital. O papel crescente que a TI tem na nossa sociedade tem chamado a atenção do Estado, e levado a um maior envolvimento dos governos nos diversos aspetos da rede (Veiga & Dias, 2010).

[50] Europol, EC3 e ENISA estabeleceram um acordo de cooperação para reforçar o apoio aos EM e instituições da UE na prevenção e luta contra a cibercriminalidade. Fora desta cooperação ficou a partilha de dados pessoais, que necessitará de uma revisão face à entrada em vigor do RGPD (Santos, 2015).

dados pessoais. A este nível, a sociedade em rede deveria subentender um controlo da mesma, no que nela circula e dos seus utilizadores, como por exemplo existir um controlo de monitorização incluindo a geolocalização, o armazenamento (‘*Cloud’ e ‘Big Data’*) e a recuperação da Informação (Inteligência Artificial). Destarte, a resposta constitucional europeia em complemento com a estratégia da UE, que pretende proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade[51], enuncia princípios da Cibersegurança, nomeadamente os valores fundamentais da UE que se aplicam tanto no mundo digital como no mundo físico (Veiga & Dias, 2010) e (Masseno,2014).

De encontro às preocupações supraexpostas, o direito nacional e internacional tem dado especial relevância à proteção dos dados pessoais, nomeadamente, quanto às questões da privacidade, da partilha e da segurança deste tipo de informações. No domínio tecnológico em que nos encontramos, não se podem descurar as possibilidades nem riscos informáticos inerentes a transferências internacionais, uma vez que se tratam de dados pessoais, facultados por cada cidadão e que, por algum descuido no seu tratamento, podem consubstanciar crimes. Este tipo de situação encontra-se previsto entre os artsº 44º a 48º do RGPD, destacando-se também o art.º 50º, que aborda a cooperação internacional neste domínio (Santos, 2015).

A presente diretiva, RGPD, aplica-se a todo o tratamento de dados pessoais realizado em território nacional, mesmo que ocorra no cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público, excluindo-se, porém, o tratamento judicial**.** A Comissão Nacional de Proteção de Dados (adiante designada por CNPD) será a autoridade de controlo nacional para efeitos do RGPD, com poderes de fiscalização, de correção, consultivos e de autorização. Esta, enquanto entidade responsável, tem tentado alertar o público em geral quanto à divulgação de

[51] “O princípio da privacidade dos utilizadores pode ser caracterizado como a guarda e a disponibilização dos registos de conexão e de acesso a aplicações da Internet, estendendo-se aos dados pessoais e ao conteúdo de comunicações privadas. Estas, devem assegurar a preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas, devendo ser disponibilizadas apenas aos utilizadores legitimados ao seu acesso” *(*Cazelatto & Moreno, 2016).

informações da esfera pessoal, no que respeita à circulação de dados pessoais pela Internet (Veiga & Dias, 2010) e (Inácio, 2017a).

Neste sentido, o RGPD vem esclarecer à luz do direito internacional, e com aplicação universal, sobre a forma como se deve proceder ao tratamento dos dados pessoais, entre outros. Aqui alertamos para a definição de tratamento[52], pois será um conceito que deverá ser integralmente compreendido e bem interpretado pelas organizações, sejam seguradoras ou PME'S, para evitar erros crassos.

No seio de cada organização, há que verificar se foram aplicados os mecanismos necessários para assegurar a privacidade dos dados pessoais, em conformidade com o RGPD, e para apurar imediatamente a ocorrência de uma violação de dados pessoais informando rapidamente a autoridade de controlo e o titular dos dados (art.º 31º). A fim de preservar a segurança e evitar que o tratamento de dados pessoais seja ilícito, "o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos associados ao tratamento e aplicar medidas[53] que os atenuem, como a cifragem". As organizações devem, portanto, adotar medidas técnicas e organizacionais, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio dos dados dos titulares, podendo incorrer em perdas e desvantagem económico-social significativa das pessoas singulares, e coimas avultadas para a empresa (crf. previsto no 83º). Logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá notificá-la à autoridade de controlo, sempre que possível, num prazo de 72 horas após ter tido conhecimento do ocorrido (art.º 33º e 34º RGPD).

[52] Segundo o art.º 4º nº2 do RGPD **"**Tratamento" diz respeito à "operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição". "Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização (…) pelos danos sofridos. (art.º 82º, nº 1); Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. (art.º 82º nº 2).

[53] Essas medidas deverão assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger.

Aqui, o RGPD cruza-se não só como sendo um elemento propulsor da necessidade crescente de existir um seguro informático que possa auxiliar ou salvaguardar eventuais despesas tidas com a gestão e tratamento de dados pessoais, tanto quando são facultados a uma empresa (numa fase inicial de recolha de dados), como também quando estão armazenados e estão sob o seu dever de vigilância. Igualmente afigurável é a eventualidade da ocorrência de um incidente informático que difunda dados da empresa e dados de terceiros.

Em paralelo, surge também a questão da aplicação real da *framework* que se objetiva, na medida em que o seu preenchimento e a completa partilha de informação conforme a mesma exige, obriga a uma exposição e transparência da empresa em si, o que pode levantar questões éticas delicadas. Contudo, julga-se ser imprescindível para a segurança da mesma, desde um fiel perfil de risco encontrado até a uma conceção de seguro mais adequada às necessidades.

Também consonante com o tema, é o tratamento de dados pessoais pelas entidades seguradoras e pela ASF-APS, estando esta última na Lei nº147/2015 de 9 de setembro, no seu art.º 32º, autorizada a proceder ao tratamento de dados pessoais considerados sensíveis nos termos do n.º 1 do art.º 7.º da Lei n.º 67/98, de 26 de outubro quando esse tratamento seja indispensável ao exercício das atribuições legais que lhe estão cometidas e à proteção dos interesses dos tomadores de seguros, segurados, participantes e beneficiários. Será uma premissa *sine qua non* para a devida aplicação da *framework* enquanto ferramenta de análise de risco.

No que respeita à figura do encarregado de proteção de dados (doravante denominado por DPO), o mesmo deverá ser designado em função dos seus conhecimentos jurídicos e tecnológicos, nomeadamente em matéria de proteção de dados, podendo exercer outras funções e atribuições desde que as mesmas não resultem num conflito de interesses[54] (art.º 37 a art.º 39º).

[54]Aqui pesa a imparcialidade da pessoa nomeada.

É ainda de destacar, conforme art.º 9º do RGPD, que "o tratamento de categorias especiais de dados pessoais, devem ser objeto de medidas de tratamento adequadas e finalidades bem definidas e específicas, a fim de defender os direitos e liberdades das pessoas singulares". Aqui é encerrada uma imposição que recai sobre as seguradoras a ter em atenção relativamente aos dados de segurados e à sua transmissão/difusão no decurso da atividade de peritagens, averiguações e outros, cruzando-se este tópico com a segurança dos dados (art.º 32º RGPD), os direitos dos titulares (art.º 12º e ss. do RGPD) e o direito de indeminização e responsabilidade (art.º 82º do RGPD).

O mesmo é aplicável para qualquer empresa que, por exemplo, queira realizar um seguro informático e tenha de acautelar previamente todas estas questões, quer empresas/clientes como companhias de seguros, serão responsáveis pelo tratamento dos dados internos e a que têm acesso em função do ramo e contrato celebrado (art.º 24º e ss. do RGPD).

Por fim, importa realçar a tão mais recente Lei nº46/2018 que estabelece o regime jurídico da segurança do ciberespaço, e, que visa garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. Explana também a estrutura e as competências do Conselho Superior de Segurança do Ciberespaço, e das equipas CERT, e, prevê ainda requisitos de segurança e notificação de incidentes. É totalmente enquadrável no âmbito da análise de risco, e deverá ser do conhecimento das empresas este regime, na medida em que devem ser cumpridos os vários pressupostos previstos, caso contrário poderão incorrer em infrações ou contraordenações, cuja fiscalização e sanções cabem ao CNCS[55].

[55] À semelhança com o RGPD, cuja entidade fiscalizadora é a CNPD.

4. Relação Interdependente do cliente/empresa e seguradora

A atividade seguradora não funciona sem o cliente, i.é., sem qualquer cidadão particular e respetivo património como também empresas e multinacionais que se apoiam, recorrentemente, em apólices de seguros. Como tal, será fundamental compreender a ótica interna das empresas, em termos de risco informático, segurança e gestão de carências, já que nos focamos no tecido empresarial enquanto potencial cliente dos seguros informáticos (Biener *et. al.* 2015).

É óbvia a relevância de considerar planos de contingência e conhecer o risco informático, pois caso contrário não sairão prejudicados apenas os dados e informações das empresas, mas também o tempo de paralisação que daí pode derivar (perdas de lucros cessantes)[56]. Também o grau de complexidade aumentou consideravelmente tornando mais difícil a administração do risco e proteção, para manutenção da segurança (Tenzer & Sena, 2004).

Assim, procura-se dissecar a interligação entre o cliente (empresa) e a seguradora (fornecedora de serviço) por forma a compreender o melhor equilíbrio na relação contratual de ambas, num sinistro de nova era. Esta análise serve não só de ponte para alcançar os resultados do presente trabalho como também aprimorar a necessidade de consciencialização das seguradoras e das empresas quanto à fusão do cibercrime/incidentes informáticos e dos seguros. Para tal, destacar-se-á aspetos críticos do risco informático, entre outros correlacionados (ACS, 2016).

[56] Como exemplo, segundo um estudo da *Eletronica Data Systems*, sobre a capacidade de respostas das empresas em Manhattan, frente ao corte de energia elétrica que sucedeu em 13 de agosto de 1990, apurou-se que afetou mais de 1000 companhias, com 320 centrais de rede das quais 100 ficaram completamente paralisados. Somente 25% destas empresas estavam, na altura, preparadas para lidar com este tipo de sinistros – riscos elétricos- e tiveram capacidade para, em 24h, recuperar o serviço informático. Os restantes 75% sem capacidade de reação, estiveram cerca de 3 dias para recuperar o serviço na sua totalidade.

4.1.Na ótica da Empresa/Cliente

Presentemente, enfrentamos muitos desafios como a globalização, a turbulência dos mercados financeiros, o terrorismo internacional, os riscos de crises ecológicas, informáticas, entre outros, o que obriga a uma revisão do conceito de Segurança Interna e a novos quadros de referência nos planos sociológicos e políticos. Isto também se aplica, por inferência, no setor privado, já que o ciberespaço e as novas tecnologias trouxeram poder a todos os agentes: indivíduos, empresas e Estados (Santos & Guedes, 2015).

O mundo dos negócios tem-se tornado mais vulnerável do que nunca às ameaças virtuais pois as suas informações transitaram do papel para o computador. Conforme já referido em capítulos anteriores, cada vez mais se torna imprescindível aplicar na cultura da organização uma estratégia[57] e planeamento geral, valores, procedimentos e políticas que envolvam a componente securitária, principalmente a nível tecnológico e das ligações virtuais, pois todas as atividades de uma organização envolvem riscos deste nível (Bonet, 2012).

Segundo Mueller (2012), há apenas dois tipos de empresas: aquelas que foram *"hackeadas",* e aquelas que irão ser". E até as próprias empresas estão a convergir numa única categoria: empresas que foram *hackeadas* e aquelas que o serão novamente. O mercado está aquém das expetativas para esta nova linha de negócios, sendo a cobertura que o acompanha, ainda residual, com um fraco percentual de empresas que compraram um seguro informático.

Muitas empresas estão focadas em gerirem e segurarem os riscos informáticos por eles próprios, dentro da sua própria organização, o que é compreensível. Contudo, as trocas comerciais com outros parceiros são massivamente eletrónicas e, tendencialmente, procurar-se-á uma extensão de garantia, enquanto seguro para

[57] As estratégias de proteção mais eficazes passam, assim, por uma abordagem delineada consoante a natureza da informação que precisa de proteção, motivo pelo qual algumas empresas conduzem auditorias periódicas para identificar o tipo de propriedade intelectual, fazendo a sua catalogação/inventariação, até para poder ser facultada para efeitos de atualização de seguro (Brown, 2005).

cadeias de negócio, pois mesmo que uma companhia esteja segura e confiante nos seus controlos de TI, haverá sempre exposição, ainda que mínima, através dos seus parceiros, fornecedores e prestadores de serviço. As empresas precisam de entender as suas próprias exposições e proteções[58], pois o caráter sempre evolutivo do risco informático é muito tenebroso e as leis recentes em termos de proteção de dados e ciberspaço, constituem-se como desafios ao crescimento deste setor do mercado segurador. Há muita capacidade no mercado, mas ainda não há um entendimento total, pelo que haverá segmentação e especialização de mercado[59] (Dobie, 2015).

As empresas podem ter requisitos semelhantes, mas díspares no que respeita ao tipo de negócio e nível de proteção necessário contra várias perdas, pelo que cada organização deve tomar a iniciativa de compreender completamente o nível existente de requisitos de proteção, antes de se envolver no processo de solicitação de seguro.

É, assim, imperativo que qualquer aquisição de seguro informático seja investigada minuciosamente antes de qualquer decisão tomada. Se o seguro obtido não for o mais apropriado, a empresa pode ficar vulnerável a responsabilidades, o que, numa componente prática e de conhecimento em campo, já se verifica com frequência[60] (Drouin, 2004).

4.1.1. Análise, Exposição e Gestão de Riscos Informáticos – Risco e Segurança no Negócio

A componente do risco e da segurança empresarial está enraizada com a gestão de riscos corporativos e tem origem a partir do tratamento dos seguros como cobertura

[58] Apesar da sua crescente relevância para as empresas atuais, a pesquisa sobre o risco informático é bastante limitada. Alguns documentos podem ser encontrados no domínio da tecnologia, mas quase nenhuma pesquisa foi feita no domínio de risco e de seguros. O denominado *"cyber insurance"* não deixa de ser frequentemente discutido e de ser uma oportunidade de mercado, devido ao aumento da consciencialização pública e da crescente exposição ao risco (Biener et. al., 2015).

[59] Os comentários fornecidos pelas empresas que não adquirem este seguro, devem-se a: a) limitação de mercado e coberturas das apólices; b) o custo das mesmas; c) a falta de transparência das coberturas (não são claras); d) a dificuldade em quantificar e o processo de subscrição; e) a falta de informação para tomar decisões adequadas; e f) problemas entre o corretor/mediador e a empresa/segurado (ENISA, 2012).

[60] Muitos segurados apenas se apercebem das falhas de seguros (produto contratado) quando surge um sinistro, ou após a regularização de um processo de sinistro. A maioria das vezes ficam descontentes com as exclusões vigentes, franquias, limites aplicados e apuramentos de acordo com as condições da apólice.

e proteção frente aos riscos operacionais[61]. Em todo o tipo de empresas, existe um potencial de sucesso e impactos que podem configurar-se como oportunidades para conseguir benefícios (aspeto positivo do risco) ou, pelo contrário, as ameaças para a sustentabilidade do êxito empresarial (aspeto negativo do risco). Por este motivo, hoje e cada vez em maior medida, a gestão do risco aborda várias vertentes, sendo esta aptidão estratégica, chave para assegurar o equilíbrio da empresa. Procura-se aqui um enfoque multidisciplinar na gestão de riscos inerentes a uma empresa ou organização, admitindo que esta gestão face a uma abordagem abrangente, permite obter benefícios através da supervisão e avaliação de inter-relações dos riscos – (ver Tabela X, Figuras 5 e 7 em apêndice (ponto 9.3)) (Fraguio & Macías, 2011).

No que concerne às principais carências de uma organização, e de encontro à sua resolução deve-se identificar os riscos específicos da organização (mapear as formas mais prováveis de se verificar uma ocorrência numa empresa, trabalho conjunto de elaboração de cenários e simulações, criação de planos específicos para mitigar riscos, planos de resposta atualizados e testados com regularidade), promover a consciencialização de riscos e regulamentos "*cyber*", e, manter aprendizagens (tais como esforços atenuantes no caso dos seguros informáticos) (Lloyd's, 2016).

O risco informático é um risco não convencional e discreto, tal como o terrorismo, incidentes nucleares, danos ecológicos (larga escala industrial), etc. É lógico supor que as empresas com uma grande quantidade de informações armazenadas em meios digitais estão mais expostas ao risco de violações informáticas. Como exemplo, os bancos têm afirmado que um único ataque informático poderia interromper as operações de toda a instituição, o que demonstra a gravidade da ameaça e a necessidade de cobertura por um seguro informático. As instituições bancárias não só possuem uma imensa quantidade de informação financeira e confidencial[62], como

[61] Ver tabela I e tabela III em anexo (ponto 8.1).

[62] "Informações a partir das quais um indivíduo pode ser identificado ou contatado de forma única e confiável - incluindo, o nome, endereço, telefone, número, saldos e históricos de contas - e "quaisquer segredos comerciais, dados, fórmulas, registos ou outras informações de terceiros que não estejam disponíveis para o público em geral" (Anderson, 2013).

também fazem muitas transações/operações online, aumentando a probabilidade do risco (European Comission, 2016).

Muitas vezes, os riscos estão correlacionados e envolvem-se em classes distintas. Uma taxonomia de riscos informáticos operacionais pode ser uma mais-valia a aplicar nas empresas, os riscos advêm de ações de pessoas, falhas tecnológicas, de sistemas, em processo internos, ou, eventos externos – tal como considerado, mais adiante, na *framework* proposta (Cebula & Young, 2010).

O risco informático também pode emergir se, no seio de uma empresa, não existir resiliência adequada ao fracasso (humano ou não humano), no ambiente virtual e nas tecnologias disponíveis. O cenário informático em rápida mudança exige processos de gestão de alterações cada vez mais robustos, para garantir que os serviços continuem disponíveis e atendam às expectativas dos clientes. No mundo atual, isto geralmente significa que a recuperação dos sistemas e normal restabelecimento da atividade, em horas ou dias não é suficiente, pois os serviços devem ser capazes de recuperar em tempo útil (Kitching *et. al.*, 2014).

É, portanto, compreensível o porquê de ter de se alocar recursos para diminuir o risco de exposição até um nível aceitável. Mas, existirá, na verdade, um risco aceitável? Haverá risco mínimo ou risco razoável? Acredita-se que não, pois todo e qualquer risco mínimo, é um risco real. O risco residual é o risco mínimo além do qual não podemos acautelar, e portanto, resultante do imprevisível. Já o risco razoável, é aquele que de facto não pode ser aceite, pelas potenciais consequências que comporta, pois, uma vez aceite, constitui-se como o risco mínimo, que pode ser admissível pelas empresas, desde que se tenha a correta noção do mesmo bem como das possíveis implicações e consequências. Por forma a correr o menor grau de risco possível, deve ser ponderada a aquisição de um produto de seguro contra riscos informáticos. Este seguro é uma ferramenta de gestão para reduzir o risco de perdas financeiras

associadas a violações, o que irá também afetar o nível de risco mínimo[63] (Gordon *et. al*, 2003).

Importa referir que, os riscos informáticos, não constituem um estatuto jurídico especial, ainda que se possam aplicar, no seu tratamento, ordenamentos como as leis em matérias de seguros. O que justifica indicar estes riscos como um fenómeno jurídico a ter em especial atenção, é a complexidade dos problemas que se levantam na prática (González, 2017). Atendendo ao exposto, referem-se três aspetos que se consideram essenciais e para os quais as empresas devem estar preparadas, nomeadamente: a) reunir um conjunto de procedimentos de resposta à crise (sinistro informático), comunicando a ocorrência (consequências) aos clientes e atualizando os seus sistemas de TIC; b) gerir os danos à reputação, através de relações públicas, publicidade e atividades de *marketing*; e c) implicações de regulação, cooperando com uma investigação/ resposta a mudanças, que remeta para regulamentos como o RGPD (Lloyd's, 2016).

O desafio é saber se as etapas para gerir os riscos informáticos são compreendidas. Embora o foco, inicialmente, tenha sido a prevenção total, agora há uma necessidade de se concentrar na resiliência, com vista à melhor deteção e capacidade de lidar com eventos inesperados (informáticos e criminais), quando e sempre que estes se verifiquem (Kitching *et. al.,* 2014).

4.1.2. Gestão e Cenarização do Risco

A dinâmica em que muitas empresas se veêm imersas implica um esforço diário. A administração do risco passa por gerir os recursos da empresa de forma a alcançar um determinado nível de exposição. Isto permite estabelecer um grau consoante o tipo de ativo, e assim permite uma menor exposição quanto mais crítico for o ativo. Este

[63] A melhor opção para lidar com o risco mínimo será transferi-lo para um seguro. O seguro permite que as organizações suavizem pagamentos para eventos incertos em custos periódicos previsíveis, através de um contrato ou cobertura específica. A adoção de investimentos em segurança é um poderoso mecanismo de incentivo que empurra as entidades acima do limite para um estado desejável, seguindo uma dinâmica de autoproteção, corroborada pela existência de seguro informático (Bolot & Lelarge, 2008).

processo (de administração do risco)[64] é um processo contínuo, em que é necessário avaliar periodicamente os riscos identificados e a exposição aos mesmos. Ao consultar as figuras 5, 7 e 8 em apêndice (ponto 9.3), poderá observar exemplos de processos/*guidelines* a adotar por empresas, enquanto matriz de risco informático e onde se visualizam as interligações dos elementos identificados, matriz esta que deverá ser atualizada periodicamente (Tenzer & Sena, 2004).

Após a identificação e avaliação dos riscos (cada empresa – de acordo com as suas caraterísticas – deverá identificar os seus), o risco informático deve ser gerido e controlado. Para tal, diferentes ações podem ser realizadas como a eliminação, redução, assunção financeira e transferência dos riscos para um terceiro, através de fórmulas do setor segurador ou financeiro (San José-Marti, 2013).

Da interpretação realizada a várias matrizes de risco, para um melhor conhecimento interno da empresa, seja por autoavaliação como também para fornecer um panorama mais específico perante uma seguradora onde se pretenda segurar um risco informático, será pertinente aplicar uma bateria de testes, e/ou questionários, tais como os representados em apêndice (ponto 9.4), nas figuras 10, 11 e 12 que abordem vários pontos pertinentes como as transações eletrónicas, a avaliação de medidas preventivas implementadas, um prospeto da apólice de seguro informático, entre outros (Adeleke *et. al.*, 2011).

Na gestão de riscos, a fase do diagnóstico[65] é um método para conhecer de forma precisa e quantificar os riscos a que a organização está sujeita, bem como as

[64] Várias fases da administração do risco: a) controlar o risco é fortalecer os controlos existentes, ou agregar novos; b) eliminar o risco é eliminar o ativo relacionado; c) compartilhar o risco é onde se inserem os seguros, com acordos contratuais é transferido parte do risco, ou a sua totalidade, a um terceiro (companhia seguros); e d) aceitar o risco é determinar que o nível de exposição é adequado (Tenzer & Sena, 2004).

[65] É aquela que "reúne e analisa os dados necessários para avaliar os problemas de natureza diferente com os quais a organização se depara em termos de riscos. Requer a realização de testes precisos para detectar os problemas relacionados com os riscos, determinar as suas chaves, o comportamento previsível, bem como a probabilidade de ocorrência e a intensidade do dano na hipótese de ocorrência do evento prejudicial indesejado". Como ferramenta de diagnóstico uma organização deve ser capaz de estabelecer uma exposição real aos riscos, identificando os mesmos e estabelecer, em termos quantitativos e qualitativos, os riscos totais e os riscos mínimos (San José-Marti, 2013).

consequências económicas dos riscos e dos sinistros. Para tal, deve contar-se com fontes fidedignas de informação, tanto internas como externas, sem esquecer o ambiente sociológico, físico e económico em torno da empresa e que influencia os riscos (San José-Marti, 2013).

No que concerne à gestão do risco de segurança da informação[66], este é um desafio para as empresas e para os formuladores de apólices por vários motivos. Primeiro, as empresas, cujas informações confidenciais precisam de proteção, compartilham riscos correlacionados devido a tecnologias comuns e à interconetividade de computadores. As empresas conduzem os seus negócios por meio de redes públicas compartilhadas e, além disso, a infraestrutura de TI das empresas é dominada por algumas tecnologias, que expõem muitas empresas às mesmas vulnerabilidades, levando a riscos correlacionados (Ögüt *et. al.*, 2011). Segundo, as empresas têm uma vulnerabilidade significativa ao risco informático, não tanto relacionado com as medidas de autoproteção[67], mas sim com a natureza inter-relacionada dos sistemas de informação, explanada nos ciclos representados nas figuras 4, 6 e 7 em ponto 9.3 do apêndice**.** Isto pode dificultar a descoberta de perpetradores do crime/sinistro, o que também aumenta a relutância de um investimento a este nível, levando a uma seleção adversa[68] (Biener *et. al.*, 2015).

Enquanto ferramenta de auxílio, e disponível para certificação avulsa, existe uma infinidade de padrões internacionais de normalização que podem servir para a gestão de riscos informáticos, na família dos ISO/IEC 27000x, *Cyber Security Best Pratices*

[66] O termo "segurança da informação" significa proteger os sistemas de informações contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de fornecer, integridade, confidencialidade e disponibilidade (Cebula & Young, 2010). Algumas orientações que se destacam para uma correta gestão de riscos informáticos, são por exemplo: a) estabelecer um compromisso organizacional; b) ter uma gestão de riscos efetiva; c) ter diálogos de risco com funcionários; d) adquirir certificação; d) manter uma monitorização continuada; e e) ponderar a transferência de risco (seguro informático como meio eficaz) (Eling, & Schnell, 2016, a).

[67] Essencialmente, o seguro é um mecanismo poderoso para promover mudanças em toda a rede e levar as empresas a um estado desejável, com investimento deliberado em autoproteção (Bolot & Lelarge, 2008).

[68] A seleção adversa é um problema que se manifesta no seguro informático pela probabilidade de se verificar uma violação de segurança. Para proteção destas situações, as seguradoras tipicamente exigem uma auditoria previamente à emissão do contrato seguro (Gordon *et. al.*, 2003).

(ENISA), entre outros[69]. Com a oportunidade de serem certificadas em conformidade com estes padrões, as empresas podem assim ter um padrão de segurança de TI e uma certificação na sua implementação, o que cada vez mais é exigido por parceiros de negócios e clientes (padrões mínimos de segurança). Especialmente as empresas que procuram uma cobertura de risco informático nas seguradoras, precisam de ter tal certificação ou a seguradora, por si, teria de conduzir uma avaliação de risco semelhante (Eling & Schnell 2016).

Este conjunto de práticas recomendadas recai também sobre o estabelecimento, implementação, manutenção e melhoramento contínuo do sistema de gestão da segurança da informação[70]. Estes padrões, para além de fornecerem uma estrutura para políticas e procedimentos que incluem todos os controles legais, físicos e técnicos envolvidos nos processos de gestão de riscos de informações de uma organização, também elencam vários requisitos técnicos como de documentação, divisões de responsabilidade, disponibilidade, controlos de acesso, segurança, auditoria e medidas corretivas e preventivas, aplicando um processo de gestão de riscos e dando confiança às partes interessadas de que os riscos são geridos adequadamente. Uma certificação deste tipo, ajuda as organizações a cumprir com vários requisitos legais e regulamentares, relacionados com a segurança das informações.[71]

O risco verifica-se consoante a sua intensidade/severidade e a sua probabilidade/frequência. Deve ser catalogado um conjunto de indicadores para monitorização periódica – ver figura 7 e tabela X em apêndice - interna e externa, para o controlo e gestão de riscos identificados. Existem muitas fases de latência,

[69] Como exemplo, para a identificação do risco temos a ISO / IEC 27005: 2011 que fornece diretrizes para a gestão de riscos de segurança da informação (suporta os conceitos gerais especificados na norma ISO / IEC 27001 e foi concebido para ajudar na implementação satisfatória da segurança da informação com base numa abordagem de gestão de risco). Outro bom indicador de risco pode ser também sob a forma de uma autoavaliação.

[70] Também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação adaptados às necessidades da organização. Os requisitos são genéricos e devem ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.

[71] Retirado de: https://www.iso.org/home.html

onde o risco se verifica e poderá pronunciar-se a qualquer momento sem preparação prévia, pelo que devem ser tomadas medidas urgentes (Bonet, 2012).
Destaca-se ainda que o cenário de risco informático está em constante mudança e, por isso, é importante que a estrutura seja suficientemente dinâmica para permitir que os cenários[72] sejam atualizados regularmente (Kitching *et. al.,* 2014).

Face à identificação, administração, gestão e cenarização do risco, consoante a forma preferível de lidar com o mesmo as empresas podem, por um lado, optar por transferir o risco para uma companhia de seguros ou, por outro lado, assumir o risco internamente por autosseguro/seguro próprio (investimento interno a usar em caso de perdas), ou também por proteção própria (atenta a redução de probabilidades de ocorrência de perdas). O seguro informático é uma solução mais viável[73] porque: a) as seguradoras tomam uma posição/interesse proativo; b) reduzem os prémios de seguro com a expansão deste mercado; c) pressionam as empresas de *software*/outras a fornecer produtos "seguros" consoante as exigências do mercado, ou a assumir as responsabilidades com garantias válidas (Mukhopadhyay *et. al.,* 2013).

Assim, não pode cair em esquecimento que os riscos coabitam continuamente com as tarefas diárias de qualquer empresa, e estão sempre latentes, mesmo quando não são identificados ou não se fazem esforços nesse sentido. Por isto, independentemente das ferramentas utilizadas pela administração de riscos, o mais importante é ter consciência que esta deve ser uma atividade prevista e levada a cabo para o funcionamento seguro dos SI (Tenzer & Sena, 2004).

[72] No seio de uma empresa, identificar e avaliar cenários de ameaça é difícil, contudo, fazer este tipo de simulações, ajuda a avaliar os riscos e tomar decisões. "O seguro informático não substitui a segurança robusta de TI. No entanto, tem um papel importante como parte de uma estratégia holística de gestão de riscos, criando uma segunda linha de defesa para mitigar incidentes informáticos" (Dobie, 2015).
[73] Outros motivos que privilegiam a escolha por um seguro informático, são: a) permitir uma redução do tamanho da perda, é mais atrativo na transferência de riscos financeiros particularmente no que respeita a riscos de terceiros; b) é uma melhor opção no caso de resultarem altos custos de transação associados às regras de responsabilidade c) pelos padrões de segurança impostos pela regulamentação (ENISA, 2012).

4.1.3. Segurança da Informação e Violação de Dados

Em prol de uma segurança consciente, necessária, focada e bem direcionada será natural que as organizações procurem uma salvaguarda nos confrontos empresariais e nas vulnerabilidades da segurança na informação. Hoje, a importância da segurança da informação adquiriu um peso tão elevado, que atingiu a lista de prioridades a nível da administração e CEO's de qualquer empresa.

Nesta senda, não poderia deixar de se mencionar os novos regulamentos, nacionais e internacionais, que aumentaram consideravelmente a consciencialização sobre o risco informático, especialmente em relação à cobertura informática por responsabilidade (para com terceiros). O mercado dos EUA é dominado principalmente pela cobertura de terceiros, enquanto as poucas apólices informáticas que já existem na Europa se concentram mais na cobertura de primeira parte (própria empresa). Entretanto, na UE estão a ser introduzidas obrigações de relatórios, enquanto novas abordagens regulatórias (como é exemplo as consequências da implementação do RGPD [74]), o que será certamente um importante fator no desenvolvimento do mercado europeu de seguros informáticos (Power & Forte, 2007) e (Lloyd's 2016).

Sem dúvida que o RGPD[75] veio aumentar o nível de interesse no mercado segurador informático, visto que as empresas devem agora ser mais abertas na partilha de dados e informar, preparar e documentar o ambiente da empresa, antes de solicitar uma proposta de seguro informático. O nível geral de entendimento das empresas ao risco informático é básico, no entanto tem havido um reconhecimento crescente das organizações e dos grupos de liderança de que o *cyber* é um risco operacional que

[74] "O RGPD é um normativo complexo, que atribui fortes responsabilidades às empresas relativamente à proteção dos dados dos seus colaboradores e clientes, exigindo a implementação de rigorosos procedimentos de recolha, tratamento e acondicionamento desses dados". As empresas irão necessitar de um *Data Protetion Officer (DPO)* para garantir a aplicação do regulamento, como acautelar prazos de conservação da informação, assegurar que são cumpridas as regras de tratamento desses dados, entre outros. Estas medidas podem afetar a empresa, na aplicação de coimas, pois há a suscetibilidade de serem comunicadas violações que podem não ser concordantes com o interesse da entidade (Inácio, 2017a).

[75] O RGPD tutela a imposição de proteção de sistemas face a acessos ilegítimos, e é um regulamento que consagra direitos fundamentais de privacidade para os consumidores, como "o direito de ser esquecido" e o direito de se opor às atividades de criação de perfis, que as empresas devem cumprir (Inácio, 2017a).

deve ser profundamente abordado e, pode constituir-se assim como o ponto de viragem para um novo modelo securitário no seio das empresas (ENISA, 2016).

Neste seguimento, a maioria das empresas não se encontra preocupada com uma violação de dados no futuro. Alguns empresários associam que pode haver impactos, mas que não levará à perda de clientes ou relações comerciais. Outros, por sua vez, encontram-se já com planos de proteção e contra violação de dados, tendo a plena consciência das desvantagens de um incidente deste tipo (Lloyd's, 2016).

Posto isto, devemos olhar para a (in)segurança intrínseca de uma empresa, pois as violações de segurança abalam muito o mercado, apesar de ser recuperável. Para isso, devem ser feitos: a) "testes" como modelos macroeconómicos de entrada/saída que avaliam a sensibilidade das economias nacionais ao ciberataque em setores específicos; b) técnicas econométricas; c) retorno sobre análise de investimento em segurança; d) caracterização da tomada de decisão no mundo real; e e) *frameworks* de gestão de risco entre outros métodos (ENISA, 2012).

Para além do suprarreferido, seria pertinente ter em atenção que, quando o risco se torna realidade e a segurança de uma empresa é violada, muitas vezes esta é incapaz de provar a uma companhia de seguros, a sua perda/violação[76]. Consequentemente, além das perdas tangíveis incorridas por uma violação, uma parte significativa da perda é intangível[77], como perda de reputação e inteligência competitiva. Outra razão pela qual uma empresa não espera receber remuneração integral das seguradoras de perdas decorrentes de violações de segurança, é porque as empresas geralmente não conseguem detetar a invasão em tempo útil. Como a autoproteção e medidas tomadas no cerne de uma empresa, não são diretamente observáveis, a gestão de riscos só pode ser melhorada pelo complemento do seguro (ÖGÜT *et. al.*, 2011).

[76]As empresas raramente se sentem voluntariamente compelidas a transmitir dados sobre intrusões pois os incentivos estratégicos não se alinham com a divulgação de ataques informáticos (Shackelford, 2012).

[77] Segundo opiniões do tribunal, este determina que as escutas telefónicas e dados informáticos (em suporte digital) são propriedade tangível, uma vez que os dados têm valor permanente e foram incorporados à natureza corpórea da empresa. Consequentemente, a incapacidade do seguro tradicional para lidar com novas ameaças informáticas cria a necessidade de desenvolver produtos de seguro especificamente projetados para cobrir os novos riscos da Internet, contando com dados tangíveis e intangíveis (Majuca *et. al.*, 2006).

É, por isto, fulcral ter noção das cifras negras[78] existentes, quando entidades que não reportam incidentes, com o objetivo de preservar a sua reputação no mercado, não transparecem as razões de muitas das intrusões nos seus sistemas. Isto reflete-se num anonimato, numa não-reação e posterior impedimento de desenvolvimento de uma boa base estatística do fenómeno[79] (Fitzpatrick & Dilullo, 2015).

Na maioria dos casos, a segurança da informação é reativa, em que só após um ataque, seja ele bem-sucedido ou na sua forma tentada, é que são implementadas novas medidas para prevenir que o evento se torne recorrente. Isto comporta o grave fator de que um ataque pode ser cometido e permanecer indetetado por um longo período de tempo. Concernente à natureza da informação, a mesma sendo privada ou confidencial, pressupõe maiores barreiras, já que não está livremente disponível a pessoas externas ao serviço, pelo que deveria estar sujeita a proteção legal ou moral. A propriedade intelectual é da empresa e deve ser mantida em sigilo.
Qualquer violação ou replicação da informação digital pode permitir a sua difusão, venda ou "resgate", estando intrinsecamente envolvida com os métodos da sua captação e transmissão externa/pública. Nestas situações, a investigação pós-incidente, deve incidir na descoberta dos intuitos associados, na medida em que, o que está em causa não é o fato de a informação ser privada, mas sim o propósito para o qual essa informação vai ser empregue, tornando-se o foco de particular interesse (Crane, 2005).

Por este motivo, será de considerar que qualquer organização ou empresa deva ter certo tipo de certificações[80] para ser aceite perante uma companhia de seguros como já fora referido. Para além disto, e especialmente importante na avaliação por uma

[78] Por cifras negras entende-se o não conhecimento e/ou divulgação dos crimes, não há uma efetiva participação dos mesmos o que dificulta as medidas da sua mitigação (Azevedo, 2016).
[79] "Os lesados ou vítimas são muitas vezes empresas, bancos, seguradoras e entidades financeiras que preferem não apresentar queixa às autoridades e resolver o problema internamente absorvendo as perdas com receio de que tal ataque, a ser conhecido, leve ao seu descrédito e perda de reputação/confiança junto do mercado. Isto naturalmente causaria prejuízos superiores ao ataque sofrido, o que é agravado nas situações em que pode haver responsabilidade legal, pelo dever de proteção de dados confidenciais" (Dias, 2012).
[80] Especificamente, a ISO 27001:2013 deverá ser uma autenticação obrigatória na medida em que, são examinados sistematicamente os riscos de segurança, projeta e implementa controlos e adota um processo de gestão abrangente, proporcionando uma abordagem holística e baseada no risco da informação segura, permite uma revisão independente da informação e considera problemas internos e externos.

seguradora previamente à aceitação do risco, demonstra ainda a credibilidade para as partes interessadas, o *status* de segurança de acordo com critérios internacionalmente aceites, cria uma diferenciação de mercado, e, uma vez certificada, a empresa é aceite globalmente, tanto no mercado interno da UE como noutras extensões. Ora, tudo isto fornece naturalmente confiança e transparência a um segurador, sendo um ponto a favor na aceitação do risco e posterior contratação de um seguro informático.

Paralelamente a esta questão jurídica de regulamentações e de proteção contra violações de dados[81], os potenciais clientes interessados em subscrever uma apólice de seguro informático concentram-se em medidas para evitar perdas negativas das consequências de uma violação, ao invés de se concentrarem nas causas, o que se constitui como práticas de segurança precárias. Do ponto de vista da cibersegurança, estão a ser identificados os sintomas dos problemas, e não as causas. O seguro informático acaba por servir não diretamente para os ataques informáticos em si, mas sim para as perdas secundárias que poderão advir.

Os motivos que parecem estar a impulsionar o mercado são: a) a privacidade; b) o alívio dos custos pós-violação; e c) o risco de reputação. Estes podem incluir multas, sanções, danos, liquidações e custas judiciais de um titular de dados ou de um órgão regulador. Muitas exigências subentendidas nas novas regulações jurídicas, fazem com que as empresas tenham uma descrição de seguro relevante nesta área, pelo que o seguro informático muitas vezes serve apenas para comunicar ao mercado a informação (ilusória) de que estão a ser geridos adequadamente os riscos informáticos na empresa em questão (ENISA, 2012).

Contudo, as empresas demonstram ter confiança nas medidas de segurança informática que possuem e sentem-se complacentes com a sua resiliência a ataques informáticos. É quase impossível as empresas estarem 100% seguras, pelo que deveria haver uma validação e testes rigorosos antes de adquirirem um sentimento de

[81] Será imprescindível saber analisar se a empresa tem ou não um programa de segurança da informação atualizado, adequado e em vigor, bem como diretrizes internamente estipuladas para tal. Devem também ser avaliadas a maturidade, perfil de risco e resiliência informáticas da empresa, e garantir as disposições adequadas para a segurança de dispositivos móveis (*gadgets*) e teletrabalho**.** (ENISA, 2016).

confiança quanto ao seu nível de preparação. É essencial manterem-se sempre atentas e regularmente atualizadas em termos de planeamento estratégico, de defesa e ofensivo, no caso de uma ameaça emergir (Lloyd's, 2016).

A dimensão (empresarial) não importa, pois, quase dois terços de todos os ataques direcionados atingem PME's, sendo um tipo de risco e ataque que afeta uma globalidade de organizações (Krickhahn, 2015). As pequenas empresas[82] são cada vez mais visadas porque podem fornecer um *backdoor* para empresas com sistemas mais robustos. Independentemente da magnitude da empresa em questão, os criminosos informáticos tendem a direcionar os ataques para empresas com menor nível de segurança (não necessariamente bancos, grandes marcas, entre outros).

As empresas precisam, portanto, de ter clareza quanto ao impacto que um incidente destes poderia ter na sua cadeia de suplementos, bem como custos de contratação de advogados, especialistas em TI, peritos forenses, e profissionais em relações públicas para resolver quaisquer problemas daí resultantes (Dobie, 2015).

Igualmente indispensável será definir uma equipa de resposta a situações de crise e manter exercícios regulares neste sentido. Também as camadas superiores, da administração, devem ter conhecimento sobre tudo o que se passa na organização, de forma transversal e transparente. Deve haver reuniões e comunicação com frequência de todo e qualquer incidente, evento de segurança e questões de risco informático, e principais ativos valiosos (ENISA, 2016).

Para além das fragilidades já enunciadas, será ainda importante ter em atenção o facto da componente técnica e fator humano enquanto potenciais riscos para as empresas, porquanto se traduzirem como variáveis diretamente relacionadas, e em contacto direto com o risco informático.

[82] Será de considerar como possibilidade que as empresas menores (entre 50 a 250 funcionários) não tenham a consciência nem recursos para uma cabal proteção informática, enquanto que as grandes empresas têm deseconomias de escala devido à complexidade. "Possivelmente, as empresas menores são menos conscientes e menos capazes de lidar com o risco informático, enquanto que as grandes empresas podem pecar pela complexidade e número de colaboradores (Biener et. al., 2015).

4.1.4. Cibersegurança e a Incorporação de Seguros Informáticos

Já lá vai o tempo em que, quando havia um problema na rede e falhas decorrentes de um ataque digital, as empresas e funcionários promoviam uma desconexão total, desligando todo e qualquer equipamento da rede, de forma frenética e alarmante. Não será esta defesa, por reação, que enaltecerá os pilares da segurança informática de uma empresa, mas sim um combate proactivo e precedente, por prevenção, que passa pela associação a um seguro informático, entre muitas outras remodelações virtuais internas. "As empresas estão posicionadas em diferentes quadrantes numa matriz (de risco) de maturidade[83] em inovação digital e segurança informática". Há uma série de *trade-offs* que as empresas fazem, que podem, potencialmente, levar a perdas diretas ou indiretas relacionadas com a cibersegurança (Nelson, 2016).

O tecido empresarial está, agora, alerta e preocupado em proteger as suas informações prioritárias, manter a integridade das suas bases de dados e assegurar acessos oportunos. Contudo, dado o aumento de vulnerabilidades associadas, os executivos procuram novas ferramentas adicionais para gerir os riscos associados à segurança da informação. Aqui surgiram as apólices informáticas, especialmente concebidas para proporcionar cobertura contra perdas relacionadas com intrusões na rede, e falhas decorrentes do uso da Internet (Gordon *et. al.*, 2003).

Não sendo este um processo direto e de solução imediata para todos os problemas informáticos e falhas tecnológicas de uma organização, o risco deve ser bem compreendido, antes de transferido ou seguro. As empresas não investem menos em medidas de segurança pela presença de uma apólice informática, simplesmente o comportamento empresarial é reforçado por ser solicitada uma reavaliação periódica por parte da seguradora (ENISA, 2016).

Algumas empresas estão a começar, então, a perceber a importância estratégica, a longo prazo, de abordar a segurança informática como um valor central e apercebem-

[83] A maturidade do risco (ou maturação) está relacionada com a natureza do risco que é entendido, e, com a quantidade de risco que é "aceitável" – risco mínimo (Nelson, 2016).

se disso como uma vantagem competitiva. Apenas 13% das empresas acreditam ter encontrado o equilíbrio certo entre as duas prioridades (lucro e segurança) e estão a verificar, um impacto na inovação imposta pelas atividades de segurança informática. Também está claro que, algumas empresas assumem riscos em demasia, muitas vezes sem perceber, enquanto outras podem não estar a aproveitar da melhor forma as oportunidades de inovação para a tecnologia disponível, descurando certos valores (Nelson, 2016).

Sublinha-se pontualmente que, ter procedimentos e apólices de segurança de rede é uma das várias etapas para alcançar a cibersegurança. Algumas ideias como a sugerida na figura 8, em apêndice para mitigar o risco informático, são, por exemplo: a) identificar os principais ativos em risco e pontos fracos da empresa, como fatores humanos, ou dependência excessiva de terceiros; b) criar uma cultura de segurança informática e uma abordagem *"outside the box"* para lidar com riscos; c) implementar uma resposta/plano a crises ou incidentes de violação de segurança e testar os mesmos; e d) tomar decisões sobre riscos a evitar, aceitar, controlar e/ou transferir (Dobie, 2015).

Da ótica do segurado, isto é, da empresa/cliente, a incerteza do risco representa um risco real, tendo quatro hipóteses para o gerir: a) evitar o risco (passa por não ter dependência de computadores, máquinas conectadas à rede ou presença de qualquer ligação à rede[84]); b) reter o risco (decisão sobre o que será mais rentável absorver qualquer perda internamente, ou porque outras opções de gestão de risco são inacessíveis[85]); c) mitigar o risco (mitigar riscos usando processos estratégicos e técnicos, que envolvem investimento em pessoas/dispositivos para identificar ameaças e preparar contramedidas com melhoria contínua dos processos de segurança); d) transferir o risco por uma taxa[86] (como por exemplo: prémio de seguro – isto permite que uma empresa suavize os prejuízos que possam resultar de

[84] Para algumas organizações isso é viável, no entanto, para a maioria das empresas, isto não é economicamente possível (Majuca et. al., 2006).
[85] Manter o risco é, por vezes, a única opção, devido à falta de recursos financeiros (idem).
[86] O seguro informático é uma das opções complementares de gestão do risco de uma empresa (idem).

sinistros/cibercrime imprevisível, como também de custos periódicos previsíveis) (Majuca *et. al.*, 2006).

Perante todas estas ameaças, complexidades e dificuldades em gerir os riscos, um seguro informático pode fornecer proteção frente a empresas com risco de ataques informáticos, ciberataques e as consequências negativas que derivem dos mesmos. Os ataques informáticos têm capacidade de atingir qualquer tipo de empresa, independentemente do seu tamanho, relevância ou sector. Este tipo de seguro pode dar cobertura a vários riscos, desde que moldável a cada caso, e a cada realidade empresarial (Iruena, 2015).

Deste modo, a agregação deste tipo de seguro/modelo de risco não pode ter uma dependência linear em conta, sendo a análise de cenários uma ferramenta mais válida neste caso. Posto isto, dado que as informações sobre o nível de proteção de segurança são geralmente conhecidas, as seguradoras podem ter que tomar decisões sob incerteza, aquando de uma solicitação de proposta de seguro informático, motivo pelo qual são promovidas as auditorias prévias à realização do seguro (Majuca *et. al.*, 2006) e (Eling & Schnell, 2016).

4.1.5. Aquisição e Vantagens do Seguro Informático

Desde sempre que as empresas se apoiam em seguros para protegerem perdas decorrentes dos seus negócios, principalmente prejuízos decorrentes de fogos, inundações e outros fenómenos da natureza. Contudo, tais apólices tradicionais não cobrem expressamente novos riscos da Internet, o que resultou em disputas dispendiosas entre as seguradoras e segurados, motivo pelo qual estes danos (puramente informáticos) recaem sobre as exclusões das apólices.

Existe ainda uma perceção (falaciosa) de que os seguros já existentes cobrem os riscos informáticos, pelo que as empresas não se movem no sentido de os obter. Contudo, também a vertente da oferta não consegue segmentar o mercado de forma eficiente e suficiente, pelo que será necessário separar os produtos específicos, por

coberturas[87], contrariamente às apólices tradicionais (Majuca *et. al.,* 2006) e (ENISA, 2012).

A transferência de um risco para uma seguradora[88] é um mecanismo de redução do risco. A incorporação de apólices de seguros nas empresas (como exemplo de raciocínio para tal ponderação, observar figura 9 em apêndice) conduz a um nível de risco onde a sua posição é assumível, pois há: a) uma retenção voluntária de riscos; b) um grau de franquias assumidas (autosseguro); c) um grau de adequação dos montantes contratados nas apólices analisadas, em relação ao risco assumido pela empresa; e d) concorrência de seguro e excesso de garantias contratadas (San José-Marti, 2013).

Paralelamente, as empresas podem recuperar uma variedade de custos graças ao seguro informático, quer seja quando são responsabilizadas como também quando os seus sistemas internos são utilizados para atacar servidores de outras empresas, ou até quando há tempo de inatividade da empresa, por ataque virtual. As organizações precisam de garantir que os orçamentos de segurança são suficientes para suportar as necessidades atuais, mas também para estabelecer um plano de longo prazo à medida que a tecnologia avança (Drouin, 2004).

De encontro à aquisição destes seguros (informáticos), as empresas contratam-nos através de corretores que, interpelam por apólices que melhor atendam aos requisitos de proteção das organizações, e que melhor se adaptem às necessidades das

[87] Existem coberturas de riscos disponíveis como: a) difamação comercial; b) dano a reputação ou desacreditação de um produto; c) invasão, intrusão, infração ou vulnerabilização de direitos à privacidade; d) violação de direitos de autor; e) extorsão comercial, vulnerabilidade ou debilitação da marca; f) alteração, cópia, destruição corrupção, eliminação ou danos a dados; g) roubo de dados (incluindo usurpação de identidade); h) transmissão de códigos maliciosos ou vírus informáticos; i) divulgação não autorizada de informações ou dados; j) negação de serviços e perca de dados pessoais. E também se mencionam possíveis extensões de coberturas como: a) danos que o segurado se possa ver obrigado a assumir por atividades próprias; b) restabelecimento de dados e perdas de receitas; c) violações de segurança e privacidade sofridas pela própria rede informática (*intranet*); d) gastos em defesa e gestão de crises devido a materialização de um risco informático; e e) sanções civis e/ou administrativas ou multas seguráveis por lei e impostas por um órgão regulador oficial ou pela administração (como é o caso da CNPD, ASF, etc.) (Iruena, 2015).

[88] São fatores a considerar na transferência de riscos: a) determinação de níveis de risco desejados e assumidos; b) capacidade financeira; c) tipo de atitude anterior ao risco; e d) estimativa de perdas. Esta alternativa requer, para a sua implementação, profissionais especializados, mas também uma visão global, que permita às empresas encontrar soluções adequadas para cada um dos problemas que possam surgir (Fernández, 2007).

mesmas[89]. Todos os requisitos têm, contudo, de ser bem compreendidos e detalhados, caso contrário, a organização pode subscrever uma apólice que não serve à sua proteção imediata para as exposições a riscos informáticos. A realização de uma autoavaliação permite que a empresa identifique e considere, sistematicamente, os problemas de segurança tecnológica, presentes e futuros (Drouin, 2004).

Outro aspeto distintivo do seguro informático, é que os riscos enfrentados e respetivas coberturas contratadas são muitas vezes exclusivos de uma indústria específica ou até mesmo da própria empresa, exigindo uma grande customização na redação de apólices. A dimensão da empresa, base de clientes, tipo de dados recolhidos e armazenados, são fatores determinantes dos termos e preços da apólice. As apólices de seguro informático são típicas no campo de terceiros (como responsabilidade por privacidade, por segurança de rede, propriedade intelectual e outras violações), enquanto que as coberturas de primeira parte (com foco na própria empresa) estão no campo da gestão de crises, interrupção de negócios, proteção de ativos de dados e extorsão informática – (consultar tabela II, em anexo 8.1) (Eling & Schnell, 2016).

Ainda em relação à aquisição de seguros informáticos, deve ser sublinhado que estes: a) são de um conhecimento limitado por parte dos líderes empresariais; b) fornecem não só uma indeminização, como também peritos consultores; c) tratam-se de apólices diferentes das usuais, desde custos legais e forenses para identificar a causa e os responsáveis do sucedido; d) acarreta mais custos de notificação, interrupção da atividade, mais apoio empresarial na identificação de riscos e vulnerabilidades; e) ajuda a proteger balanços empresariais; f) eleva padrões de segurança informática; g) mitiga riscos e probabilidades de ocorrência; h) promove a identificação, tratamento e determinação de um perfil de risco da empresa; e i) ajuda a enfrentar o desafio que o risco informático representa, construindo uma metodologia crucial de avaliação do risco (Lloyd's, 2016).

[89] "As empresas têm recorrido cada vez mais ao seguro contra riscos informáticos para gerir melhor a ameaça do cibercrime, e qualquer responsabilidade legal resultante de violações de dados (Shackelford, 2012).

Em suma, a posse de um seguro informático não só é uma chave protetora para as responsabilidades das empresas, como também, em caso de batalhas legais ou em sinistros graves, acaba por reduzir a carga de custos com litígios. A gestão e mitigação de riscos, é fundamental para garantir que a infraestrutura corporativa mantenha um alto nível de autoconservação e, o seguro é vital para esse processo**.** Desta forma, é legível a emergência na modernização de mentalidades, políticas e procedimentos, que exige a atualização de sistemas para minimizar vulnerabilidades e que dote as empresas com um sistema de registo de dados fidedigno, seguro e adaptado às necessidades do negócio (Drouin, 2004).

4.2. Na ótica da Seguradora

Estamos na vanguarda de uma nova fronteira de tipologias de seguros. Há que ter em conta que um elemento comportamental interessante neste contexto é o otimismo latente que muitas pessoas demonstram em relação ao risco informático ("isso não vai acontecer comigo", "os meus dados não são interessantes o suficiente" ou "a minha empresa tem um bom informático"). Identificar os fatores subjacentes a esta perceção e aumentar a consciencialização, pode ajudar a amplificar a procura por um seguro contra riscos informáticos[90] (Noonan, 2011).

As seguradoras deixaram de cumprir unicamente o papel que tinham, de assumir o risco para que o património do segurado seja indemnizado dos danos que lhe fossem causados. Hoje em dia, as seguradoras devem também desempenhar um papel pró-ativo, colaborante com a administração pública e terem uma função social em matéria de prevenção e tutela do meio ambiente, tal como ocorreu nos incêndios de 2017, em Portugal. Nesta senda, temos a operacionalização e trajetória dos sistemas de socialização de riscos, sistemas coletivos de coberturas, associações seguradoras e resseguradoras (Fraguio & Macías, 2011).

[90] Hoje em dia a noção de risco informático é muito redutora, pois cada organização se foca mais no que ocorre no interior da empresa, sendo certo que os riscos informáticos não são autossuficientes, havendo necessidade de expandir horizontes a alargar fronteiras delimitativas do risco. Enquanto que a confiança da sociedade na Internet, cresce exponencialmente, o controlo cresce linearmente (Healey, 2014).

Segundo Ralph (2017), ao contrário do seguro automóvel ou patrimonial, o seguro informático não é um produto padrão com um conjunto de recursos básicos de dimensão singular. Este tipo de seguro será diferente para cada empresa. O mercado, atualmente, é dominado por apólices de violação de dados, que cobrem empresas pela perda de grandes lotes de dados, geralmente dados de clientes. Uma apólice informática *standard* pagaria despesas de crise, como peritos técnicos, despesas de notificação (do cliente) e ajuda nas relações públicas, bem como no ressarcimento de lesados (terceiros). A cobertura oferecida está, portanto, a aumentar, especialmente quando se trata de potenciais perdas de receita.

O mercado segurador irá agora prender-se com a incorporação do RGPD[91] e a Lei de Segurança no Ciberespaço, o que aumentou o sentimento de alerta e foco no aspeto da segurança de dados, da informação e da cibersegurança. Isto porque, interfere diretamente com as operações comerciais das seguradoras, e, os reguladores, acionistas e clientes irão usar tal argumento para responsabilizar as empresas por maiores níveis de segurança, levando também ao acionamento de mais verbas/cláusulas. Por outro lado, ao trabalharem com parceiros especializados, como advogados, especialistas em TI e seguradoras, as empresas podem entender melhor os riscos que enfrentam e ajudar a mitigá-los a fim de proteger os seus balanços patrimoniais (Lloyd's, 2016).

Em relação à atualização da indústria dos seguros informáticos, esta tem vindo a amadurecer, passando-se de apólices primitivas e limitadas para uma maior gama de produtos com coberturas substancialmente mais altas. As seguradoras têm também mostrado que são capazes de lidar com questões de implementação, apesar das dificuldades inerentes. Estas, através dos seguros informáticos, podem reunir conhecimento sobre riscos, identificar vulnerabilidades em todo o sistema de empresas, exigir auditorias de pré-qualificação e adotar estratégias pró-ativas de

[91] Com o RGPD a instalação de CCTV em casas, empresas ou entidades públicas, vai deixar de ter qualquer controlo prévio. Particulares ou empresários vão passar a poder fazê-lo sem o aval de qualquer autoridade pública, dado que a CNPD apenas irá verificar a sua conformidade *à posteriori*. A alteração enquadra-se na mudança de paradigma da proteção de dados que passará de uma lógica de controlo prévio para uma lógica de autorregulação e, assim, passará a ser da incumbência das organizações, públicas e privadas, estarem aptas a demonstrar que cumprem todas as obrigações legais (Lloyd's, 2016).

prevenção de perdas. Assim, sugerem que as empresas minimizem prejuízos usando incentivos às organizações, que afiguram o seguro informático como um dos seus interesses (Majuca *et. al.*, 2006).

É certo que o mercado dos seguros informáticos[92] precisa ainda de volume e diversificação. Será necessária mais segmentação no futuro com seguradoras especializadas em determinados setores. É claro que a falta de conhecimento é um obstáculo para o crescimento, tanto em termos de entendimento das empresas como em relação às exposições e subscrição de seguro. O seguro traz mitigação de risco adicional e compensação em caso de sinistro, mas deve ser um complemento dos sistemas de proteção e ferramentas de auxílio da gestão de risco, e não um substituto dos mesmos (Ögüt et. al., 2011).

Evidentemente, as falhas podem começar no ciberespaço, mas irão rapidamente ser transportadas para o mundo físico. Está a haver uma concentração do risco nos, e para os, sistemas *online* e, tudo o que está conectado à Internet pode ser penetrável. À medida que mais empresas se envolvem, oferecendo mais produtos, a opção de seguro informático está-se a tornar mais aliciante como uma recomendação para todas as empresas, não apenas para as que detêm maior quota de mercado. O comércio de seguros deverá, assim, corresponder à eminente procura, sendo certo que as seguradoras quererão o cliente (por vezes grandes cadeias empresariais) satisfeito, mas também se devem salvaguardar a si próprias (Healey, 2014).

4.2.1. Preparação/Evolução do mercado segurador informático

Nas últimas décadas, tem entrado em confronto o desejo de ganhar mercado e a competência das companhias de seguros[93], sem exceção, o que é fruto do crescimento

[92] Note-se que, será insuficiente, reformar o mercado de seguros atualmente imperfeito, pois tal será ineficaz para alcançar o resultado pretendido na gestão de riscos informáticos. Em vez de uma reforma, deverá ser feita uma reestruturação e mudança de linhas de raciocínio dos seguros tradicionais (Ögüt *et. al.*, 2011).

[93] Deve-se prosseguir o acompanhamento efetuado à evolução da exploração técnica das empresas de seguros, nomeadamente no que respeita aos principais seguros e especialmente naqueles em que se assumem riscos que se traduzem em responsabilidades de longo prazo, no sentido de assegurar que as políticas de subscrição, tarifação e provisionamento, são adequadas e suficientes (ASF - APS, 2018).

da carteira, e exigência de clientes, levando, por sua vez, a uma ampla diversificação, sofisticação e número de coberturas disponíveis. Com isto, tem culminado uma grave consequência: a simplificação dos quesitos necessários para aceder ao seguro, isto é, um facilitismo associado à contratação de uma apólice de seguro e à assinatura de um contrato. São indicadores deste flagelo, a rápida aceitação dos riscos, a menor informação disponibilizada sobre a apólice e a velocidade de transmissão de acidente/sinistro (Pereira, 2013).

Apesar do ceticismo de muitos CEO's sobre a mais-valia deste seguro, a verdade é que a adesão aos mesmos tem aumentado ao longo dos anos. Para avaliar qual o cenário mais provável, e como garantir que o seguro contra riscos informáticos se torne uma ferramenta eficaz para as empresas que procuram gerir ativamente os riscos, é necessário investigar como este seguro evoluiu e quais são os principais obstáculos à sua adoção contínua. O seguro contra riscos informáticos é uma ferramenta para gerir a exposição de empresas e que mitiga o risco de ataques, ou seja, apólices de seguro que cobrem perdas (derivadas, resultantes ou provocadas) por ataques informáticos e violações de dados (Shackelford, 2012).

Atualmente, o mercado do seguro informático ainda é bastante emergente e, por isso, o desenvolvimento de esquemas de cooperação nesta área é um trabalho em curso. De uma perspetiva de mercado, os seguros patrimoniais e de RC estão praticamente disponíveis na esfera comercial em todo o mundo, embora estes cubram apenas danos diretos a ativos físicos, excluindo os riscos informáticos, taxativamente, em todo o tipo de apólices. Como resposta a esta situação, um mercado especializado tem surgido, com oferta de coberturas específicas para estes riscos, de maior destaque nos EUA e agora também com alguma expressão na Europa (UK e Países Nórdicos). A nível nacional é, ainda, desconhecido ou inexistente (Biener *et* al., 2015).

Neste momento, as seguradoras têm para oferta, seguros de equipamentos eletrónicos informáticos[94] e de RC profissional[95], o que não corresponde a um *cyber insurance* no seu propósito. A concretização de uma apólice de seguro informático é bem mais complexa, e implicará um investimento de avaliação anterior e superior, como garantia de prevenção, pelo que um regulamento vinculativo de responsabilidade por violações de segurança (e outros não cumprimentos), deve ser uma pré-condição deste tipo de seguros (Böhme, 2005).

Em resumo, esta informação vem apresentar um produto inovador no mercado dos seguros[96] que surge como uma resposta direta à demanda de segurados que atualmente não têm este tipo de cobertura, e se veem preocupados com eventuais ataques informáticos. Há uma consciência crescente de que muitos setores da economia global estão, cada vez mais em risco, de ataques virtuais contra infraestruturas críticas e sistemas operacionais que podem levar a danos à propriedade e interrupção de negócios vitais (já para não falar nas consequências resultantes de eventual divulgação de dados pessoais, efeito direto do RGPD). Isso pode ter consequências devastadoras para as operações de uma empresa, e exige que estes tenham um alto nível de sofisticação de TI para se protegerem (BritInsurance, 2017).

4.2.2. Tipos de Apólices, Coberturas -Enquadramentos e Exclusões

A partir de uma perspetiva jurídica, o risco é a causa do contrato seguro que motiva o segurado (empresa) a contratar uma entidade seguradora, para obter uma cobertura que garanta um futuro sinistro. A atividade seguradora prossegue a cobertura de riscos que as pessoas, coisas ou direitos podem enfrentar antes da possibilidade de

[94] Protege/segura danos materiais a computadores fixos ou portáteis, *tablets*, monitores, impressoras, teclados, ratos e outros periféricos considerados como material informático (Ocidental, 2015).

[95] Aplica-se mais a seguros para empresas de prestação de serviços informáticos, garante erros, omissões ou negligências profissionais e reclamações de terceiros por danos ou prejuízos causados pelo segurado (RC Exploração ou RC Produtos Pós-Trabalho) no decurso do seu exercício profissional. Cobrem danos decorrentes da atividade, no decurso de trabalhos, instalações ou reparações, erros profissionais, infidelidade, entre outros (Axa, 2017) e (Hiscox, 2017).

[96] Concordantes com a opinião de Eling & Schnell (2016,a), hoje, o mercado de seguros informáticos está em estágios iniciais, mas, à medida que o seu desenvolvimento continua, as reservas de risco/informação irão tornar-se maiores e mais dados estarão disponíveis. Consequentemente, novos concorrentes entrarão no mercado, o que aumentará a capacidade de seguro e baixará os preços dos prémios. Além disso, levará a uma terminologia e padronização mais uniforme dos produtos.

serem afetados pela realização de certos eventos futuros, prejudiciais e incertos, denominados sinistros.

Apesar de tudo, as apólices de seguros informáticos tornaram-se mais abrangentes, pois as seguradoras entendem melhor o cenário de risco e as necessidades específicas dos negócios. Na verdade, as companhias de seguros estão a lidar com o que costumava ser considerado um problema intransponível (por exemplo, seleção adversa, informação assimétrica, risco moral) e que poderia levar a uma falha dessa solução de mercado. Já o seguro informático, é um instrumento ambivalente, na medida em que funciona para a seguradora que busca obter lucros de prémios que excedam as perdas a longo prazo (distribuindo o risco de eventos de perda incerta em muitos clientes independentes) e, também para o segurado (indivíduo ou organização) que procura maximizar o seu lucro, gerindo o risco de incertezas de eventos e perdas informáticas (Majuca et. al., 2006).

Logo, é imprescindível que as partes tornem muito claras e detalhadas as necessidades que pretendem cobrir e as condições objeto do contrato de seguro informático, o qual se reveste de diversas peculiaridades, desde a complexidade e multiplicidade dos sistemas, como da tipologia de serviços/utilização de redes informáticas. Só ao determinar o objeto e causa se qualificará a natureza contratual. Teremos contratos sobre bens informáticos[97], e contratos sobre serviços informáticos[98] e, atendendo à natureza dos bens informáticos, teremos contratos que recaem sobre bens materiais, o hardware, e, outros que recaem sobre bens não materiais, o software (Arien, 2003).

As seguradoras que estão a desenvolver apólices de seguro informático, deparam-se com falta de dados e de experiência e neste tipo de risco, até porque a informação

[97] Consideram-se como todos aqueles elementos que formam o sistema – computador – e todos os equipamentos que tenham uma relação direta de uso respetivo aos mesmos. Também são considerados aqueles bens imateriais que fornecem dados, pedidos, procedimentos e instruções no processamento automático das informações que constituem o elemento informático (González, 2017).

[98] Serviços de recrutamento e seleção, consultoria geral, planeamento, desenho, programação, desenvolvimento, manutenção ou implantação de sistemas (González, 2017).

sobre complicações informáticas não se encontra publicamente disponível, devido à afetação para as empresas, que tendem a nem sequer o reportar (Eling & Wirfs, 2015).

Neste âmbito, uma apólice de seguro informático pode contemplar várias verbas adicionais com coberturas[99] que são extensíveis a clientes/terceiros, como custos de notificação aos que sejam potencialmente afetados por uma violação de dados, atendimento ao cliente e eventuais custos legais associados. Também são contemplados, em algumas seguradoras, custos de investigação forense para avaliar a causa do sinistro e tecer as ilações e repercussões daí advindas (Lloyd's, 2017b).

A cobertura de perdas diretas normalmente cobre a destruição ou a perda de ativos de informação da empresa, interrupção de negócios na Internet, extorsão informática, prejuízos devido a ataques de DOS, reembolso de despesas relativas a relações públicas e até mesmo transferências fraudulentas de fundos eletrónicos. A cobertura de perdas indiretas normalmente cobre reclamações decorrentes de conteúdo da Internet, segurança na Internet, erros de tecnologia, omissões e custos de defesa para com terceiros (Majuca et. al., 2006).

Como exemplo de coberturas[100] principais e mais comuns tem-se : a) responsabilidade e custos de violação de dados - para dados pessoais[101] e corporativos, incluindo custos de notificação, custos forenses de peritagem técnica, custos de resposta incluindo requisitos de notificação, monitorização de crédito, *call centers* [também conhecido como cobertura de ativos de informação (cobre danos/roubos dos sistemas e hardware do segurado), podendo cobrir custos de reparação ou recriação de dados furtados e/ou corrompidos]; b) responsabilidade por privacidade e segurança de rede – para sistemas invadidos ou comprometidos, incluindo ataques de negação de serviço; c) perdas resultantes de apropriação indevida de propriedade intelectual ou informações comerciais confidenciais; d) responsabilidade relacionada com os media – para

[99] Resumidamente são cobertos danos físicos e não físicos, tais como: a) extorsão; b) regulação; c) interrupção de negócio; d) danos à reputação da organização; e) responsabilidade (para com terceiros); f) violação de dados e g) avaliações e custos/multas com dados de cartões de pagamento (Lloyd's, 2017 a).

[100] É dado enquadramento sempre que a empresa segura mantenha os níveis de sistema de segurança iguais ou superiores àquelas que se verificaram à data do início da apólice em questão (Majuca *et. al.*, 2006).

[101] Dados pessoais são por exemplo (números de CC, NIF's, telemóvel, cartas de condução, moradas, matrículas, etc.) e informação de saúde - são os tipos de dados mais expostos (ENISA, 2016).

publicações digitais; e) interrupção de negócios/da rede – perdas de rendimento causadas por interrupção de rede e negócios devido a um incidente informático (seja código malicioso, ataques DOS, acesso não autorizado ou outros); f) custos de restauro de dados e programas – resultantes de uma ocorrência de interrupção de negócios informáticos; g) comunicação de crise – para mitigar danos à reputação; h) cobertura contra roubo na rede – com base no furto de fundos; i) responsabilidade regulatória – multas e penalidades legais cobertas/custos de resolução e defesa contra violação de regulamentos; j) extorsão e gestão de crises (pagamentos para prevenir perdas de rede e evitar a implementação de uma ameaça); l) responsabilidades para com clientes, e custos legais associados aos processos por violação das suas informações privadas[102] - (consultar também tabelas II (anexo 1), figura 1 e 2 (anexo 2)) (Allianz , 2017).

Enumeram-se também algumas das mais comuns exclusões, tais como: a) qualquer ato que viole ou cuja omissão venha a violar qualquer lei, sendo um limite da apólice quando tal seja ilegal -as suas consequências não se encontrarão cobertas - ; b) danos resultantes de qualquer divulgação de informação empresarial ou interna à organização[103]; c) danos em códigos informáticos, ou seja, fatos, conceitos ou informações convertidas em formas utilizáveis para comunicações, interpretações ou processamentos por equipamentos eletrónicos; d) erros na configuração de operações informáticas, nem quaisquer custos com atualização de sistemas ou ativos digitais, à exceção de custos de restauração; e) falhas de interrupção de perda de uso, acesso ou redução/alteração na funcionalidade de precisão, disponibilidade ou programas eletrónicos; f) qualquer apreensão ou destruição de ativo digital ordenado por autoridade governamental, tributária ou judicial; g) perda ou aumento derivado de lei/portaria que regule a atividade ou que seja diretamente imputável ao mesmo; h) perda/dano por roubo, arrombamento ou furto causado por qualquer pessoa que participe no mesmo (exemplo: furto de computador de colaborador, com dados da

[102] Custos derivados de obrigações legais ou sanções por incumprimentos, custos de "resgate" se um terceiro exigir pagamento para se abster publicamente de divulgar/causar danos aos dados confidenciais de uma empresa, perdas financeiras por perda de clientes e cessação de contratos daí decorrentes (Anderson, 2014).
[103] Considera-se informação interna à empresa: a) segredos comerciais b) patentes; c) listas de clientes; d) informação financeira, de cartões de crédito ou qualquer informação não-pública.

empresa) – (consultar também figura 1 em anexo (ponto 8.2)) (Anderson, 2014) e (Allianz, 2017).

Há, ainda, a referir outra adicional e notável característica dos seguros informáticos nomeadamente coberturas restritas destinadas a atingir diferentes tipos de consumidores. Outro raciocínio é que, ao definir a cobertura mais especificamente, os seguros informáticos são capazes de se envolver na diferenciação do produto e, assim, oferecer produtos a mercados específicos. Como tal exemplificam-se três produtos de seguro informático, com respetivas exclusões e extensões de enquadramentos, em diferentes seguradoras[104] (Majuca et. al., 2006).

Uma vez providenciados exemplos em vigor, bem como destacadas as principais coberturas, enquadramentos e exclusões de apólices informáticas, há a registar, no entanto, falta de clareza quanto a certas coberturas, como sendo uma das razões pelas quais as empresas não adquirem seguros informáticos. Muitas vezes, as apólices contêm várias exclusões, havendo uma grande gama de incidentes que, dificilmente serão cobertos, como acima ficou explícito[105].

Assim, demonstra-se o que se tem vindo a referir desde o início: que as apólices de seguros informáticos são bastante complexas, não só por haver um grande número de exclusões associadas, como também devido à natureza do próprio risco ser muito dinâmica. Isto culminará numa incerteza tanto para a seguradora[106] como para o segurado, quanto ao que a apólice de seguro informático realmente cobre, dado que o objetivo principal é que a mesma funcione, sempre que for necessário ou que se verifique um sinistro que justifique a sua ativação. Pressupõe-se que as várias coberturas suprarreferidas forneçam uma salvaguarda para perdas resultantes de um ataque perpetrado por uma ampla gama de causas[107], já que as apólices

[104] Para tal, deverá ser consultada a figura 1 em anexo (ponto 8.2).
[105] Consultar figura 2 anexo, para detalhe e descrição técnica de tipos de ataques informáticos.
[106] Importa também realçar que, pela complexidade, novidade e cariz dinâmico do seguro informático, poderá ser uma limitação ou ameaça legal para corretores de seguros e agências de mediação pois será difícil dar uma previsão especifica da cobertura/capital. A incerteza jurídica sobre o que será e o que não será considerado um risco informático segurável, pode ter um efeito negativo no desenvolvimento do mercado (Biener et. al., 2015).
[107] Embora seja possível determinar o que aconteceu e quando, é muito difícil determinar quem causou o ataque. É identificado o ativo afetado e localizado o vetor de intrusão (Noonan, 2011).

convencionais[108] são frequentemente omissas quanto à cobertura de perdas causadas por incidentes informáticos (Noonan, 2011) e (Biener et. al., 2015)

Destarte, apesar das diferenças encontradas na classificação de crimes informáticos e respetivas condutas, é certo que estes são comportamentos antijurídicos, não autorizados e não éticos relacionados com o processamento e/ou transmissão de dados. O alvo dos seguros informáticos é, não só, o que se constitui como crime informático, mas também, incidentes de cariz informático. Assim, em matéria informática, convém estabelecer amplas coberturas que se adequem ao alcance do negócio/atividade em si, à tipologia de uso de tecnologias e também à preparação técnica dos operadores (mapa de pessoal), sempre concernente ao que se afigura como potencial risco informático (Lima, 2017). Como por exemplo, se se verificar um sinistro informático[109] que comporte consequências financeiras, estas devem ser apreciadas por forma a perceber se se trata de um dano de equipa, se foi uma perda de fiabilidade no tratamento de informação e/ou se provocará danos a terceiros (Arien, 2003).

4.2.3. Processamento seguro: Declaração inicial e aceitação do risco

A forma como um seguro informático é concebido, subscrito e aplicado a uma empresa não é por si só um processo automático, o que obriga a uma dedicação exaustiva no processo de análise inicial trazendo, desde logo, vantagens aquando da sua triagem. Contudo, também os pressupostos sendo morosos e dependentes de várias condicionantes, obrigam a uma observação próxima mais rigorosa (consultar *Client-Reaches Insurer Workflow* (Figura 13) e *Insurance Request Processing Workflow* (Figura 14), em ponto 9.5 do apêndice).

[108] Apresentam cláusulas desatualizadas e que não estão minimamente desenhadas para providenciar proteção de risco informático, e idealizarem um perigo tão moderno como um ataque informático (Noonan, 2011).
[109] O qual pode também ser equiparado, não exclusivamente, a um "ciberataque entendido como uma sequência de ações destinadas a produzir um resultado não autorizado ou uma perturbação indesejada na confidencialidade, integridade ou na disponibilidade de um serviço ou produto, ou seja, a proteção do ciberespaço é perspetivada numa lógica de mercado e de continuidade de negócio" (Bravo *et al.*, 2012).

4.2.3.1. Mais valias *versus* Pré-Requisitos do seguro informático

Uma seguradora somente redigirá uma apólice informática se as medidas adequadas de mitigação de risco estiverem em vigor, todas as condições reunidas e a seguradora puder verificar a eficácia dessas ferramentas nas avaliações iniciais. Essas avaliações, também ajudarão a aumentar a consciencialização sobre o risco informático, constituindo uma ação proveitosa para a empresa. Neste tipo de seguros, devem ser conduzidas análises de cenário, acompanhando o desenvolvimento tecnológico (computação em nuvem, IoT, tecnologia de cadeia de blocos - *cryptocurrencies*, etc.). Também é importante que as seguradoras limem as suas próprias habilidades analíticas, criem o conhecimento necessário de segurança de TI e sejam mais resilientes neste aspeto ou aproveitem, então, a competência de empresas especializadas para tal (Eling & Schnell, 2016).

Na ótica da análise prévia que a seguradora deverá implementar *à anteriori* da realização de um seguro informático, deve-se, em primeiro lugar, perceber qual o grau de exposição de uma empresa o qual será sinalizado por um número de indicadores de risco. Assim, é medida qual a propensão mínima para a perda de risco por incidente informático, também de forma a que a seguradora conheça o cliente com que está a estabelecer um vínculo contratual, e se a probabilidade de risco é elevada ou minimamente controlável. Em segundo lugar, todas as informações capturadas por qualquer uma das empresas *outsourcing* de consultoria/auditoria[110] sobre o estado de maturação da empresa, serão usadas, unicamente, para entender a perda sistémica e limitar hipóteses ou prever eventos de origem desconhecida. Será importante fornecer uma avaliação do potencial de risco e perdas, testando vários componentes da empresa, com revisões iniciais e periódicas, enquanto precauções

[110] Dado que, uma parte extremamente importante da oferta de produtos do setor segurador na venda de apólices e subscrição de contratos seguros, é a base de conhecimento e análise aprofundada do seu cliente, e, certos tipos de avaliações de risco não podem ser feitos internamente pelas seguradoras, será de recorrer a *OutSourcing*, para estabelecer uma confiança a esse nível. Muitas consultoras e auditoras irão reconhecer e controlar riscos relacionados com as TI (relativo a segurança de informação e infraestruturas de TI), manter conformidade com os principais padrões de segurança e exigíveis a certa gama de empresas (PME's) sendo crucial uma avaliação de ativos, adequação e vulnerabilidades dos SI das empresas (BritInsurance, 2017).

securitárias. Isto poderá ser submetido, por exemplo, em informações de subscrição e relatórios trimestrais (BritInsurance, 2017).

Em termos de portefólio das seguradoras sobre riscos informáticos, estes têm vindo a solidificar-se, trazendo ofertas adicionais, como avaliação de risco e investigação de violação de dados. As melhorias na avaliação do risco ao longo do tempo, permitem cobrir mais riscos o que, por sua vez, pode resultar na introdução de apólices que cubram até danos físicos - quando associados a um incidente induzido por motivo informático. As participações de sinistro têm aumentado, o que acaba por ser um *feedback* evolutivo e positivo do mercado segurador informático, dando força ao mesmo, associado à descoberta das causas de sinistro (ENISA, 2016).

Concernente à forma como um contrato de seguro informático[111] é estruturado, esta difere da forma como é utilizado pelos gerentes das TI de uma empresa, ou seja, são exploradas as decisões por detrás de uma divulgação de sinistros informáticos. Por isto, acresce a estas apólices, para além do princípio da boa-fé, a transparência na contratação**.** Neste sentido, selecionam-se alguns dos pré-requisitos que devem constar na fase de subscrição: a) um modelo referência de "quantificação de custos" do *Cyber Attack*; b) diretrizes e estratégias rigorosas em caso de incidente informático; c) uso extensivo de terceiros, especialistas do setor (quer na avaliação de risco, cálculo de impacto financeiros, como na gestão do risco e deteção da origem do ataque); d) análise contínua de portefólio para definir a exposição particular (da própria empresa) e sistémica (terceiros envolvidos) (Bandyopadhyay *et. al.*, 2009).

Naturalmente que, qualquer produto de qualidade vem com um preço e, qualquer prestação de serviço ou contratação de um seguro informático também encarecerá o orçamento. Falamos aqui de custos[112] aquando da compra de uma apólice, e não

[111] Atualmente, os contratos oferecidos pelas principais seguradoras são orientados à arquitetura (como uma violação de rede), baseados em ativos (como a violação de dados), específicos do ataque ou focados em assunção de responsabilidades que derivem de um sinistro informático. (Bandyopadhyay *et. al.*, 2009).

[112] Há pelo menos quatro razões para o elevado custo das apólices: a) a novidade do produto e, portanto, o pequeno tamanho dos "pools de risco" e do número de participantes no mercado (disponibilidade limitada); b) os dados limitados, fazendo grandes carregamentos de risco (des)necessários; e c) assimetrias de informação significativas, que exigem verificação de estado dispendiosas e avaliação de risco inicial. Os prémios para este tipo de seguros são atualmente altos, especialmente para PME's, mas relativamente moderados, considerando as grandes incertezas envolvidas **(**Biener *et al.*, 2015).

custos cobertos pela mesma aquando da verificação de um sinistro, *à posteriori*. Esta nova natureza e evolução do risco informático, apresenta uma série de questões que precisam ser abordadas, especialmente em torno da compreensão dos custos associados a um sinistro informático. Isto exige uma abordagem diferente para a avaliação do risco informático, por analogia com os tradicionais riscos de seguro[113] (Kitching *et. al.*, 2014).

Perante uma análise precoce da seguradora quanto ao risco informático[114], é necessário caracterizá-lo e controlar a probabilidade da sua realização[115] desde uma perspetiva objetiva. Também numa ótica mais ofensiva e proactiva, com capacidade de fazer frente ao risco, deve-se reconhecer o mesmo e saber tratá-lo estrategicamente, diferenciando-os pela tipologia, implicações e patamar de gravidade. Sendo esta uma premissa indiscutível, a conexão entre risco e responsabilidade deve ser abordada adequadamente pois o risco é próprio do âmbito de toda a atividade económica, de tal forma que vai pré-determinar o marco de responsabilidade do operador/utilizador (Fraguio & Macías, 2011).

Em quatro etapas, pode-se formular um plano de seguro informático que inclui: a) conduzir uma auditoria de riscos de segurança da informação; b) avaliar a cobertura atual; c) examinar apólices disponíveis; e d) selecionar uma apólice. O primeiro passo é realizar uma auditoria completa do atual risco de segurança da informação[116], sendo das fases mais cruciais. O seguro depende muito de avaliações autenticadas, para evitar fraudes e outras questões. Isto proporciona maneiras eficientes de medir e

[113]As organizações devem alavancar a sua própria experiência no desenvolvimento de práticas para aumentar a resiliência do risco informático, e para desenvolver produtos de seguro informático que estejam alinhados com a estratégia de negócio, o que exige equipas multifuncionais. (Kitching *et. al.*, 2014).

[114] As seguradoras devem ainda a) melhorar as áreas de pré-avaliação de risco antes da subscrição de apólices; b) investir/antecipar o cálculo do risco acumulado; c) considerar a adoção de padrões e metodologias comuns; d) introduzir sessões explicativas, através de cenários e exemplos gerais das coberturas da apólice informática; e e) esclarecer o "idioma" da apólice e oferecer um processo de subscrição transparente. (ENISA, 2016).

[115] Um segurador assume um risco informático pois: a) apesar das consequências serem arriscadas e amplas, a ocorrência de sinistros é relativamente pequena; b) as organizações também têm mais atenção e investem mais na segurança pois têm todo o interesse em reduzir o risco de uma quebra de rede ou intrusão maliciosa; c) pode aceitar o risco desde que quantificável e com um limite superior; e d) os riscos de uma falha ou ataque são independentes de outros tipos de riscos conexos. (Mukhopadhyay *et. al.*, 2005).

[116] Apesar da consciencialização imposta pelo RGPD, relativa a regulação das violações de dados do setor privado, cada vez mais os tribunais estão dispostos a responsabilizar as empresas e entidades públicas por não protegerem informações privadas (Shackelford, 2012).

relatar métricas de segurança, exigindo uma melhor rastreabilidade dos eventos - consultar *Client-Reaches Insurer Workflow* (Figura 10) (Bolot & Lelarge, 2008) e (Shackelford 2012).

A segunda etapa, passa por demonstrar que os seguros informáticos podem oferecer benefícios e resultados desejáveis identificados por analogia com outros mercados (por exemplo, seguro contra incêndio) que incluem: a) incentivos para as empresas aumentarem o nível de segurança das infraestruturas tecnológicas; b) processos para definir padrões de segurança, sujeitos a validação (como a série do ISO 27000); c) empresas de consultoria e peritagem enquanto suporte para investigar as práticas de segurança como parte do acordo contratual (seguro/apólice) e também em casos de sinistros; d) certificação de produtos/serviços de TI; e) incentivos e meios para promulgar melhores práticas; e f) incentivos para manter a responsabilidade e os custos, para lidar com alguns dos riscos de segurança informática, dentro do setor privado (ENISA, 2016).

O terceiro e quarto passos são essencialmente questões comerciais, onde também os mediadores e corretores devem ter uma consciencialização e formação integral sobre todos estes aspetos, para se revestirem de especial cuidado e dever de responsabilidade (agravada) para com o cliente. Não se poderia deixar de referir que, atualmente, presenciam-se muitos lapsos entre a forma como a apólice está feita, é explicada e exposta ao cliente, e, como esta funciona verdadeiramente em caso de sinistro, em termos de coberturas e outros. Muitas vezes, a falha de comunicação ou um desentendimento em termos de pretensões com um seguro, ocorrem junto dos setores comerciais (ENISA, 2016).

5. Framework para modelação de processos

5.1. Manifestações do Risco – Sugestão de estruturação

Como se tem vindo a compreender, uma análise de risco é fundamental para uma boa aliança "empresa-seguradora", sendo o primeiro passo para uma futura estrutura a ser aplicada em vários âmbitos. Tanto para as empresas mais desenvolvidas, como para as seguradoras, associações de comerciantes, da indústria e muito mais além, o interesse será total neste tipo de ferramenta auxiliar e complementar para uma correta avaliação de riscos. Esta ilação deriva do facto de as abordagens atuais da segurança informática serem geralmente voltadas para o passado, contudo, há uma necessidade crescente de uma abordagem holística e voltada para o futuro: uma que tenha como premissa a avaliação de riscos (que leva à mitigação e resiliência) (Kesan & Zhang, 2016).

Neste sentido, uma *framework* de risco ajudará as organizações a entender as suas condutas em relação à cibersegurança, aplicando os princípios e as melhores práticas de gestão de riscos para melhorar a segurança e a resiliência da infraestrutura crítica. Fornece, também, várias abordagens atuais de segurança informática, reunindo padrões, diretrizes e práticas que estão a funcionar, de forma efetiva, em vários setores atualmente. Contudo, esta não é uma abordagem única e singular para gerir o risco informático, sendo uma ferramenta útil para o complementar e completar, enquanto instrumento pioneiro na avaliação de risco (NIST, 2017).

O objetivo aqui, é providenciar uma ideia do cenário regulador para uma correta gestão de segurança informática nas empresas, com aplicação para a contratação de seguros informáticos associados, tendo por base perfis de risco das empresas, mais ao encontro da realidade nacional. Através deste contributo, identificam-se as boas práticas nos estágios iniciais do ciclo de vida de um seguro informático (ou seja, antes da apólice ser assinada), sendo também extensível aos processos de pedido de seguro

e tratamento após sinistro informático (conforme fluxogramas em ponto 9.5 do apêndice, respetivamente figuras 13, 14 e 15)[117] (Shackelford, 2012).

Verdade é que, as companhias de seguros deverão estar mais atentas, e em vias de incorporar e assimilar a necessidade de implementação de maiores capacidades de avaliação. Isto será necessário para determinar o estado da infraestrutura de segurança de uma organização e a sua maturação quanto ao risco informático, ao examinar uma solicitação de proposta de seguro pela empresa, e, na vanguarda desta nova tipologia de seguro (Drouin, 2004).

5.2. Delimitação de uma framework (premissas)

A construção e estruturação de uma *framework* de caráter multidimensional, reveste-se de especial dificuldade, principalmente quando se fala de gestão de riscos e de um modelo universal aplicável a todo o tipo de empresas, ramos e setores de negócio. Por estes motivos, carece de uma explicação detalhada do conjunto de processos e análises que levaram até à escolha das variáveis (métricas e dimensões operacionais), bem como argumentos que justifiquem a definição da ferramenta proposta.

Este ensaio prende-se com uma tentativa pioneira de fornecer um modelo de decisão, que auxilie tanto a seguradora quanto o segurado a decidir efetivamente sobre produtos de seguro informático, enquanto ferramenta de mitigação contra incidentes informáticos. (Mukhopadhyay *et al.* 2013).

Pretende-se, assim, criar um modelo de risco para avaliar as condições sob as quais a cobertura para riscos informáticos pode ser concedida, a qual tem o objetivo de descrever um procedimento para aplicar a apólices de seguro informático, como um instrumento de gestão de risco (Böhme, 2005) e (Eling & Wirfs, 2015).

[117] Quando um ataque informático ocorre, é analisado o sistema para se identificar qual a vulnerabilidade que foi exposta. O facto de se verificar um ataque informático, é indicativo da inadequação dos procedimentos de segurança informática na empresa em questão (Kesan & Zhang, 2016).

Este modelo que se apresenta, deriva de uma estrutura geral de gestão de riscos operacionais, nomeadamente com enfoque na célula de apólice de seguro informático (apólice de segurança informática) – (consultar tabelas I e III em anexo (ponto 8.1)). Promove uma linguagem comum entre segurança informática e pilares do risco operacional**.** Isto pode ser estabelecido, concordando-se com uma definição comum, usando estruturas a título de exemplo como as normas ISO e NIST[118], se desejado, e depois formulando um fluxograma de responsabilidades (Culp & Thompson, 2016).

Importa referir que, qualquer modelo ou estrutura esquemática terá de ser atualizada consoante a permuta de riscos, ameaças e vulnerabilidades que a empresa sofre. Permitem também facultar uma taxonomia e mecanismo de organização para as empresas, através de análises para: a) descrever a sua atual postura de segurança informática; b) descrever o seu estado de destino para a segurança informática; c) identificar e priorizar oportunidades de melhoria, dentro do contexto de um processo contínuo e repetitivo; d) avaliar o progresso em direção ao estado alvo; e) comunicar entre partes interessadas internas e externas sobre o risco de segurança informática. Tais questões acabam por ser bastante exaustivas e técnicas, sendo que será exequível um resumo geral das mesmas, sob a forma de questionários exemplificativos (figuras 10 a 12), construídos e adaptados internamente, enquanto ponte de lançamento para a *framework* desenvolvida (CheckRisk Framework – Tabelas VI, VII, VIII e IX) e também enquadrável nos processos em *workflows* desenvolvidos (Figuras 13 a 15), presentes em apêndice, respetivamente nos pontos 9.4, 9.2 e 9.5 (NIST, 2017).

Relativamente às métricas[119] , estas são ferramentas para facilitar a tomada de decisões e melhorar o desempenho e a responsabilidade, sendo que as medidas são dados quantificáveis[120], observáveis e objetivos que suportam as métricas. Enquanto ponto de partida para qualquer empresa iniciar ações de estratégia, as métricas possibilitam medir, monitorizar e avaliar os seus processos estratégicos, devendo para

[118]*NIST Framework* - (Anderson,2014).
[119]Observe-se que as métricas de interesse não estão limitadas às métricas de "segurança básica" carecendo de desenvolvimento para as atividades relevantes que enfrentam ameaças e riscos informáticos (Bolot & Lelarge, 2008).
[120] Os níveis, subcategorias e categorias de implementação, são exemplos de métricas.

efeitos de eficácia de segurança, ser usadas para identificar pontos fracos, determinar tendências para melhor utilizar os recursos (securitários) e julgar o sucesso ou o fracasso das soluções de segurança implementadas.

As métricas e medidas de segurança informática podem ajudar as organizações a: a) verificar se seus controlos de segurança estão em conformidade com uma política, processo ou procedimento; b) identificar tendências de segurança, dentro e fora do controle da organização; e c) criar significado e consciência das posturas de segurança organizacional. O estudo de tendências permite que uma organização monitorize o seu desempenho de segurança ao longo do tempo e identifique as alterações que exigem ajustes na postura de segurança da organização (Black *et. Al*, 2008) e (NIST,2017).

As seguradoras procuram oferecer uma resposta a este dilema e entrave comercial (avaliação de risco), através de uma estrutura de produto modular em que a cobertura é escolhida pelo cliente, e a intensidade da avaliação de risco depende então da modalidade/verba pretendidas. Esta afigurou-se também como uma hipótese pertinente, dado que permitiria uma modelação de processos consoante o segurado e/ou tipo de empresa**.** As dimensões modulares seriam: a) a dimensão estrutural (participantes/relacionamentos/cargos); b) a dimensão de componentes (recursos humanos, técnicos, de informação e ontológicos); c) a dimensão de funcionamento (processos, metodologias, processos complementares); e d) a dimensão comportamental (comportamentos obrigatórios, condições e restrições, acordos e cooperações) (Biener *et al.* 2015).

Constituindo-se igualmente como exemplos de variantes de análise, a maioria das seguradoras usa as seguintes informações ao realizar uma avaliação de linha de base para todos os setores e, dependendo dos resultados, uma avaliação extensa (ou de acompanhamento): a) enumeração e distribuição geográfica dos negócios (tamanho, operações e receita) ; b) detalhe nos negócios (setor, atividades, serviços, funções terceirizadas e exposição ao risco); c) dependências na infraestrutura de TI (uso, armazenamento, partilha, volume, sensibilidade a dados, - por exemplo dados

pessoais - e, responsabilidade derivada); d) histórico de incidentes; e) presença corporativa em *social media*; f) política e histórico de reclamações; e g) limite de política solicitada (ou apetite de risco do segurado) (ENISA, 2016).

Contudo, parece-nos mais direto acolher variáveis simples, e que no seu desdobramento explicativo englobem um conjunto de áreas críticas de uma empresa, pois já será o suficiente para se perceber a sensibilidade do segurado. O objetivo presente não se concentra na conceção de estrutura de modelação de processos direta, nem num quadro único de cibersegurança[121]. Pretende-se sim, sugerir uma *framework* que parta de um questionário que é cruzado com diferentes tipos de dimensões de risco (organizadas de forma mais abrangente, sem pormenorização exaustiva), numa métrica de tolerância ao risco (com base em grelha de vulnerabilidade/valor), e complementar a *workflows* elucidativos.

Tudo isto gerará um perfil de risco, qualitativo e indicador da maturidade da empresa, que por sua vez permitirá a contratação de um seguro adequado às suas necessidades. Assim opta-se por circunscrever a amostra de estudo a quatro dimensões principais do risco (informático): Pessoas, Informação, Tecnologia e Instalações (Cebula & Young, 2010) e (Culp & Thompson, 2016).

No que concerne ao cruzamento de variáveis, as mesmas permitirão chegar a um tipo de perfil de risco, cujo quadrante reflete a postura de cibersegurança[122] e a posição em relação ao risco informático da empresa alvo de análise, de uma forma direta e facilmente percetível. Como se pode entender, este quadrante de risco será apenas um primeiro passo em toda a cadeia que um seguro informático progride e se constrói,

[121] Destacam-se os cinco pilares da cibersegurança, que se constituem como os principais resultados identificados pelas indústrias, negócios e empresas como úteis para a gestão do risco de segurança informática que são: a) identificação; b) proteção; c) deteção; d) resposta; e, por fim, e) recuperação. Mais sucintamente, devem-se identificar possíveis fontes de risco, entre materiais, produtos, competência de setor , ambiente comercial, sempre com base no ciclo permanente: Avaliar, Proteger, Prevenir, Detetar, Responder (ciclo de cibersegurança) (NIST,2017).

[122] O seguro informático deve ser visto enquanto um incentivo para a cibersegurança. Com este propósito, poderia ser utilizado um observatório de ameaças informáticas, que incorporasse: a) provedores de Segurança de Sistemas de Informação (Antivírus, SIEM etc); b) redes de resposta a incidentes ; c) media especializada em segurança informática (blogs de segurança, publicações de segurança informática, etc.); d) fornecedores especializados em "*Cyber Intelligence*"; e) redes de partilha de informação específicas do setor; e f) resultados da análise interna de ameaças informáticas (Kitching. *et. Al* 2014).

embora seja uma das partes mais fulcrais porquanto se intersetar com todos os fluxogramas gerados, sendo transversal a todas as partes.

Este tipo de ferramenta, é pertinente, não só, numa auditoria primária de segurança realizada pela própria empresa (análise de risco), como na investigação do cliente por parte da seguradora (aquando da avaliação do risco) mas também após um incidente de segurança – sinistro informático – e posteriores tratamentos, nomeadamente na parte da averiguação de causas (peritagem técnica).

Assim, deve ser avaliado em que quadrante de risco a empresa se encontra para o cruzar com o perfil de risco noutros quadrantes internos. O motivo pelo qual este fator é tão relevante, prende-se com os ajustes necessários a realizar consoante o perfil de risco da empresa, para que esta se torne mais apelativa a ser segura, e o seguro informático que faça seja o mais adequado à sua dimensão estrutural, comportamental e de funcionamento.

Com isto, sugerem-se outras recomendações práticas, tais como: a) ajustar a postura de risco inerente da empresa para ver qual o quadrante mais adequado para a sua empresa a curto e a longo prazo; b) avaliar o apoio da diretoria e da liderança, pela frequência de uso, cumprimento e interatividade dos briefings de segurança informática; c) examinar práticas de medição de risco informático - perguntar se o risco é medido, com que frequência é medido, se é usado para fins de prestação de contas, planeamento estratégico, aprovação de orçamento ou quaisquer outros propósitos - ; d) verificar possíveis incentivos desalinhados na estrutura organizacional[123]; e) verificar a cultura, educação e sensibilização a todos os níveis; e f) assegurar práticas fortes de gestão de tecnologia (Nelson,2016).

A seguradora não pode exigir obrigatoriamente um relatório de avaliação de segurança, mas deve estabelecer, como pré-requisito, alguma prova de preparação informática da infraestrutura. Dar aos clientes cenários e exemplos práticos de

[123] Por exemplo, ter em atenção a formação técnica das equipas de desenvolvimento e a educação de qualquer executivo que pode ser vítima de *"CEO fraud",* bem como a demais populações de funcionários que podem ser alvo de manobras maliciosas de engenharia social.

coberturas poderia funcionar como um método rápido para aumentar a compreensão do seguro informático[124]. Há que ter em conta que estas medidas podem: a) melhorar a avaliação de risco das seguradoras, adaptando prioridades e foco; b) incluir novos itens para avaliação; e, c) melhorar a preparação do cliente, por meio de uma lista de verificação completa de avaliação de risco[125].

A *framework* funciona aqui como uma alavanca, na medida em que o seguro pode mais facilmente ser entendível e selecionado consoante os resultados obtidos, e após reflexões sérias sobre as vulnerabilidades e valores de uma empresa. Também porque o prémio é "discriminativo" do cliente que não investe em segurança, e, o seguro torna-se um forte incentivo para investir na segurança, não só informática, mas a nível transversal (em pessoas, informação, tecnologia e informações) (Bolot & Lelarge, 2008) e (ENISA, 2016).

A empresa pode, então, colaborar com os seus corretores de seguros para alocar o risco com responsabilidade e determinar, antes do contrato seguro em si: a) quais os custos do fluxo de trabalho que estarão sujeitos a cobertura; b) quais os custos de fluxo de trabalho que ficarão fora da cobertura; e c) quais os custos de fluxo de trabalho que podem não ser seguráveis. Para isto, este tipo de metodologia avalia o risco de um ponto de vista prático e experimental (Stark & Fontaine, 2015).

5.3. Composição e validação de modelo

Na construção e validação da *framework* proposta[126] - denominado *CheckRisk Framework* - optou-se por selecionar variáveis de um dos eixos de análise de acordo com o nível de tolerância que uma empresa se autoavalia, e não em termos de risco

[124] Como parte do processo de proposta, as seguradoras podem solicitar que um cliente lhes forneça detalhes das aplicações/Intranets que utilizam, sejam eles desenvolvidos internamente ou por programador externo. No caso de se tratar do último, a seguradora poderá solicitar detalhes do contrato de serviço (Drouin, 2004).
[125] Para tal avaliação deve focar-se: a) os recursos de uma empresa, e conduzir uma análise minuciosa em qualidade e quantidade; b) considerar a existência de exercícios recorrentes como um fator-chave para avaliar a integridade da resposta de um cliente ou sua preparação; e, c) analisar o envolvimento da administração nestes assuntos de segurança informática (ENISA, 2016).
[126] Ver CheckRisk Framework – Tabelas VI, VII, VIII e IX em ponto 9.2 de apêndice.

baixo ou alto, dado que esta trata-se de uma perceção errónea por parte de uma empresa. Será mais atingível uma empresa conseguir classificar se é mais ou menos tolerante a um determinado tipo de situações, porque tal grau deriva de questões internas da organização, do que pontuar o nível de risco em que incorre, pois esta é uma condicionante que, muitas das vezes, está fora do campo de controlo/sensibilidade da empresa. Para tal selecionou-se os níveis de *Tolerante, Pouco Tolerante, Intolerante* (NIST, 2017).

Em relação à justificação dos níveis de tolerância, importa explicar que: a) *Intolerante* considera-se como sendo alto o risco e nível de ameaça para a empresa, e que se encontra abaixo da média em termos de inovação tecnológica e maturidade de cibersegurança; b) *Pouco Tolerante,* considera-se como sendo médio o risco e nível de ameaça para a empresa em análise, encontrando-se alinhada com a média em termos de inovação tecnológica e maturidade de cibersegurança e c) *Tolerante*, considera-se como sendo baixo o risco e nível de ameaça para a empresa em análise, e que se encontra acima da média em termos de inovação tecnológica e maturidade de cibersegurança[127] (ACS, 2016), (Nelson, 2016) e (NIST, 2017).

Também foram selecionados fatores de risco segundo uma taxonomia operacional e direta, de forma a simplificar as variáveis, e agregá-las de modo universal num dos eixos de análise. Caso contrário seriam vários os quadrantes de análise, o que tornaria esta ferramenta demasiado pesada e dispersa na sua aplicabilidade prática. Assim sendo, determinaram-se as categorias gerais de *Acções de Pessoas, Sistemas e Tecnologias, Processos Internos e Eventos Externos*. Estes são os padrões multidimensionais (selecionados) presentes na análise da cibersegurança/risco informático (Cebul & Young, 2010), (Biener, 2015) e (Eling & Wirfs 2015).

Esta *framework* ajuda a implementar no processo de "programação" do seguro contra riscos informáticos e também ajuda, inevitavelmente, a gerir o risco de segurança da informação. Essa estrutura é baseada em todo o processo de gestão de riscos, inclui

[127] Na grande maioria das frameworks, são usados algoritmos para obtenção de resultados mais precisos e objetivos. Neste caso não, recorrendo-se apenas a estilo qualitativo. Cada caso é um caso, e alguns resultados darão acima ou abaixo da média consoante a preparação da infraestrutura de SI (Nelson, 2016).

um plano abrangente de decisão de seguro informático em quatro fatores principais de risco informático. Tais fatores devem ser examinados, para que quem leia, responda e interprete a presente *framework*, saiba a que corresponde cada parcela (ver tabelas IV e V, em apêndice) (Eling & Wirfs 2015).

A dimensão *"Ações de Pessoas"* reflete a forma como os funcionários, responsáveis e outras entidades terceiras que contactam ou interferem - direta/indiretamente - com a empresa (segurado) lidam e se defendem contra o risco e segurança informática. Válido para fraudes, sabotagem, erros, omissões, falta de capacidades técnicas, conhecimentos e outros. Nesta categoria inserem-se, por exemplo, ações deliberadas, inadvertidas, intencionais e "não-ações" (Cebula & Young, 2010), assim abrangendo o dolo, a negligência e o erro, bem como a ação e omissão.

A dimensão *"Sistemas e Tecnologias"* mede a extensão em que falhas de equipamentos e departamentos de TI ou a nível de rede interna e partilhada (Internet) podem provocar uma síncope ao normal funcionamento da empresa, e impedir o acesso e controlos, seja por exemplo de uma inativação de duas horas ou de uma interrupção de serviços de duas semanas. Também preconiza uma reflexão inevitável sobre problemas de maior envergadura, como ataques informáticos direcionados, crime informático a escala global ou violações de dados. Válido para certo tipo de especificações, configurações, definições de segurança, testes de manutenção e compatibilidade. Nesta categoria inserem-se sistemas no geral, componentes de *hardware* e *software* (Cebula & Young, 2010).

A dimensão *"Processos Internos"* avalia a extensão em que os processos de liderança de uma empresa e procedimentos internos contatam com o risco e a segurança informáticos. Reflete em que medida falhas intrínsecas à empresa comprometerão o seu funcionamento, operações, exposição e tratamento. É válido, para monitorizações periódicas, fluxo de trabalho, níveis de serviço estipulados, desde pessoal, contabilidade, formação e outros. Nesta categoria inserem-se, por exemplo, controlos de processos, processos de apoio ou de execução de projetos (Cebula & Young, 2010).

A dimensão *"Eventos Externos"* mede o volume de informações sobre ameaças e vulnerabilidades recebidas de fontes de partilha de informações (sejam derivadas de parceiros, fornecedores, terceiros com ou sem relação comercial e outros exteriores à empresa). Válido para falhas na cadeia de fornecedores, condições de mercado, litígios, conformidades regulatórias, transportes, inundações, incêndios, etc. Nesta categoria inserem-se, como exemplo, desde assuntos legais, de negócio (comerciais), dependências de serviços e catástrofes naturais[128] (Cebula & Young, 2010), (Biener, 2015) e (Eling & Wirfs 2015).

Ainda neste seguimento, e para também poder fornecer alguma consistência à análise e validação da *framework*, foi associada uma classificação quantitativa (simples)[129] a cada categoria de nível de tolerância, para assim, ser feito um cálculo simples de pontuação direta, que permitirá colocar a empresa num determinado perfil de risco, obviamente, de modo subjetivo (mas fiel à realidade dos factos apresentados e descritos ao momento da análise de risco, para efeitos de celebração de seguro informático). Acaba por funcionar como uma dupla análise, enquanto que se aplica a *framework* em si, pois é feita uma subavaliação em paralelo, embora correspondente ao grau como o tratamento das informações pode comprometer uma empresa. Para tal, identificam-se *quadrantes de <15 (como pragmático/avançado ou inovador), entre 15 e 25 (dinâmico/resiliente ou conservador) e, >25 (sensível /básico ou iniciante)*[130] (Gordon *et al.*, 2003), (ITSO, 2007), (Healey, 2014) e (Nelson, 2016).

Por fim, no que respeita às possíveis conjugações unitárias, por interseção de coluna/linha de análise estas encontram-se detalhadas, bem com as respetivas quadrículas de escolha possível em tabela VIII em apêndice, e explicadas na escala

[128] Ver conjunto tabelas em anexo 1 (ponto 8.1).
[129] Este complemento com escala quantitativa foi regulado por regras próprias, atendendo a médias gerais atingíveis. Tem também por base a grelha de valor-vulnerabilidade enquanto métrica independente (Gordon, *et al.* 2003).
[130] A gestão de risco relacionada à segurança da informação é "o processo de avaliar o risco, tomando medidas para reduzir o mesmo a um nível mínimo, mantendo-o". Assim, as organizações devem começar a avaliar as ameaças associadas aos seus SI, sendo que o valor da informação vulnerável também precisa de ser considerado neste processo. Nesse último aspeto, foi incorporada uma grelha de vulnerabilidade, métrica esta que se encontra no eixo de nível de tolerância ao risco da *framework* sugerido, por forma a transpor uma avaliação quantitativa simples, para definição de perfil de risco (Mukhopadhyay, *et al.* 2013).

quantitativa na tabela IX, associado à tolerância/vulnerabilidade da informação (ITSO, 2007) e (NIST, 2017).

Em termos de risco local e enquanto resultados possíveis da *framework* aplicada, consideramos que existem três níveis de perfil de risco nas organizações, na qual as mesmas se poderão inserir, nomeadamente: a) o *básico*[131] - também denominado por sensível ou iniciante - onde são tomadas ações simples no cerne da empresa que podem protegê-la de alguns riscos informáticos); b) o *resiliente*[132] - também denominado por dinâmico ou conservador - (onde, infelizmente, as etapas para proteção contra futuros ataques informáticos globais serão insuficientes, mas suficientes no presente); e c) o *avançado*[133] - também denominado por pragmático ou inovador - (em organizações maiores e mais sofisticadas, com capacidade de se envolverem em riscos informáticos mais complexos, e contemplarem uma melhor capacidade defensiva) (Healey, 2014).

Todas estas variáveis de análise funcionarão de modo conjugado, e em parceria, com os questionários apresentados, seguindo os fluxogramas também construídos (ver encadeamento no apêndice 5).

Novamente se reforça que, com vista a que uma *framework* não seja exaustiva, são identificados apenas os tópicos mais genéricos e abrangentes do risco informático, o que não impede que se realizem futuras versões de aprofundamento, de cada uma delas, com respetivo enfoque em áreas específicas. Existem várias prioridades dignas de análise de risco[134], contudo, numa pré-triagem de avaliação de risco para

[131] Onde se implementam: a) listas de permissões de aplicações; b) uso de configurações padrão de sistema seguro; c) *software* do sistema de correção e aplicações, dentro de 48 horas; e d) número reduzido de utilizadores com privilégios administrativos (Healey, 2014).
[132] Onde prevalece: a) a redundância; b) a resposta a incidentes e planeamento de continuidade de negócio; e c) exercícios, testes e planeamentos de cenários, entre outros (Healey, 2014).
[133] Onde se implementam: a) um alargamento do horizonte de risco; b) um seguro informático; c) uma exigência de padrões/produtos mais resilientes e seguros; e, d) uma gestão de risco a nível de topo (Healey,2014).
[134] Vários são os pontos dignos de análise, e onde o risco pode residir, tais como: a) controlos de acesso; b) consciencialização e treino; c) avaliação e autorização de segurança; d) configuração da gestão; e) aquisição de sistemas e serviços; e f) integridade dos sistemas e da informação. Contudo, isto são questões que deverão fazer parte de uma avaliação de risco à posteriori e já mais incisiva, com vista à restruturação do estado de preparação e maturação de uma empresa, relativamente ao risco informático (Boyens, *et al.*2015).

contratação de um seguro informático, não se pretende que a mesma seja demasiado fatigante nesta fase inicial do processo (NIST,2017) e (NIST, 2017, a).

5.4. Análise dos contributos estabelecidos – Limitações, Eficácia e Potencialidades

Uma coisa é falar-se de gestão de risco, e outra é falar-se do seu financiamento, sendo uma eterna dicotomia. Esta, poderá ser resolvida por duas alternativas: a) assumir/reter o risco residual; ou, b) transferi-lo (partilhá-lo), sendo certo que, é possível escolher a quantidade de risco a transferir, na mesma proporção da informação que se quer dar a conhecer ou partilhar com a companhia de seguros[135]. Os custos associados a uma avaliação deste tipo, bem como serviços e manutenções associados, constituem-se como um obstáculo à sua viabilidade na prática (Fernández, 2007).

Neste tipo de modelos e *frameworks* de risco, quanto maior o número de empresas interligadas, maior o número de interconexão e de incerteza/desvio padrão, aumentando-se o nível de risco e de impacto. As empresas com uma quantidade significativa de TI nos seus principais processos de negócios constituem, em grande parte, o lado da procura pelo mercado de seguros informáticos. Esta situação sugere que os mecanismos de mercado, por si só, podem não produzir simetria de informações no comércio de seguros informáticos. As empresas com menor intensidade de troca de informação e que pouco se apoiam nas TI, têm acesso, nas condições habituais a seguros mais acessíveis, sendo que muitas vezes nem recorrem ao mesmo, por o risco ser considerado muito ínfimo (noção de risco mínimo) (Ögüt, *et al*. 2011).

[135] Antes de se tomar uma decisão e em qualquer caso, especialmente nos seguros informáticos, deve estar a empresa sujeita a uma análise de custo-benefício. Deve ser preparado um plano de continuidade de negócios pois a instabilidade da situação informática e da segurança de informação de uma empresa, naturalmente estará sempre a oscilar e modificar à medida que o tempo vai passando (Fernández, 2007).

Enquanto demarcação a este tipo de estudo, destaca-se ainda o facto do risco ser dinâmico devido ao progresso técnico e ao uso de novos sistemas e dispositivos, mudando de forma drástica e repentina. Por este motivo, e também pela contínua mudança do nível de ameaça, dados dispersos, multicamadas de interconetividade, o assegurar do risco informático vem com uma multiplicidade de desafios – para complemento de raciocínio sobre dificuldades de segurabilidade do seguro informático e algumas limitações/problemas inerentes, consultar esquema síntese na figura 3 em apêndice. Assim, para as apólices a contratar serem adequadas a diferentes cenários, com um correto acionamento e enquadramento, devem as empresas, na sua gestão, forte e bem projetada, criar uma estrutura compreensiva do seu nível e/ou perfil de risco (Kitching et. Al 2014).

Reforça-se ainda que, apesar de muitas seguradoras tentarem acompanhar o ritmo do mercado informático, a verdade é que não há nenhuma abordagem em particular que encaixe em todas as companhias e que possa funcionar como manual universal de boas práticas. O grande desafio na codificação de um seguro informático é a interação inerente e a sobreposição com produtos padrão (Kitching *et. Al* 2014).

Para a conceção de um seguro informático, as seguradoras devem exigir auditorias de segurança da informação, como que um exame virtual e anatómico (equivalente a um exame físico e análises exigidos para uma cobertura de seguro de saúde, por exemplo). Logo este aspeto, por si só, constitui-se como um entrave, pois a empresa tem de se predispor a fornecer informações e disponibilizar dados que, interferem com a esfera mais íntima do seu negócio. Naturalmente que isto causa transtorno ao cliente, e pode ser contraproducente, na medida em que pode até não se decidir efetuar o seguro ou o mesmo não ser aprovado (Shackelford, 2012).

Infelizmente, no momento: a) não há um "roteiro" específico ou comprovado para análise; b) não há nenhum arquivo de dados empíricos estatisticamente significativos; nem c) nenhum algoritmo de quantificação para calcular o risco de ataque informático. Tanto quanto se pode criar e testar, tem-se os fluxogramas conforme os

apresentados, que facultarão um avanço na compreensão da complexidade da situação dos seguros informáticos (Mukhopadhyay, *et al*. 2005).

Acredita-se que, propor formulários extensos não será a solução, dado ser saturante para qualquer cliente que queira contratar um seguro de forma simples e célere. Mas também, a empresa pode não ser capaz de responder por si só a questões pertinentes, e que apenas uma consultora externa poderá analisar em detalhe. Assim, se os requisitos forem menores e se diminuir as necessidades, simplifica-se e resume-se de forma direta ao que é estritamente necessário. Isto terá as suas vantagens e desvantagens, como facilmente se afigura.

Contudo, ao extrair o que não será necessário, fazendo uma filtragem, cumpre reunir documentos e certificações para validar o estado da empresa, o que será perentório no contexto da realização de um novo (e primeiro) seguro informático.

Com base nisto, será possível prever, até um certo ponto, os riscos que a empresa poderá incorrer/sofrer, e está-se em condições de se submeter um seguro informático da forma correta e sem consequências imprevisíveis que prejudiquem o segurado, numa eventual indeminização de prejuízos futura (BritInsurance, 2017).

Quanto à eficácia desta sugestão, a mesma terá de ser estudada e testada, sendo facilmente aplicada a empresas várias, como por exemplo PME's enquanto estudos de caso. Apenas têm de ser transparentes, cooperantes e fiéis à sua realidade empresarial. Um modelo torna-se tão mais eficaz quanto mais simplificado estiver, pois quando são colocadas questões e medidos parâmetros, estes devem ser os mais objetivos e diretos possível. Quanto menor o grau de dúvida ou ambiguidade uma empresa tiver, mais fidedignamente esta responde. Desta forma, ainda que a *framework* concebida pareça simples e limitada, esta permitirá na verdade, atingir um perfil de risco bem sustentado, sólido e de fácil perceção sobre as suas raízes.

Assim, acredita-se que, com partida numa estrutura deste género, seja bastante mais intuitiva a passagem para outro tipo de modelos complementares, e que circunscrevam a problemática, convergindo para a mesma área de interesse, e tópicos

fundamentais que, naturalmente, um segurado deve separar e eleger para uma conceção de uma apólice informática.

Contudo, importa mencionar que a verdadeira eficácia e prováveis obstáculos ao estudo, apenas poderão ser identificados na sua concretização e aplicação práticas. Só assim se poderá melhorar e restruturar certo tipo de variáveis em análise, e/ou detetar possíveis ajustes a serem feitos à *framework.*

No que concerne às potencialidades do estudo, este, corresponde a uma etapa inicial e fundamental para a evolução de avaliações de risco e avanço dos seguros informáticos. Sendo uma ferramenta devidamente aplicada e bem-sucedida, torna-se uma mais-valia para a empresa, com potencialidades várias em termos de cibersegurança, ciberdefesa, resiliência ao risco informático, progressão do negócio e que faculta uma maior confiança em caso de sinistro.

Envolver profissionais forenses pré-enquadrados ou outros profissionais de resposta a crises (como monitorização de crédito, relações públicas, intermediário na relação com a seguradora, etc), será outra das opções. Será igualmente preferencial elaborar vários processos de triagem da avaliação de risco, por forma a torná-las mais fluidas e simplificadas, e aprofundar a análise de risco, sob a alçada da seguradora – afinal, o cliente paga o prémio, logo pretende que o seguro facilite, resolva os problemas, ou pelo menos ajude no processo (Anderson, 2014).

No entanto, no que diz respeito ao seguro informático, o paradigma de seguro tradicional da análise de risco, ainda não se aplica. Enquanto isso, as empresas propensas ao risco podem melhor entender a questão do seguro informático, não apenas compreendendo o risco crescente, mas também considerando cuidadosamente os fluxos de trabalho que normalmente ocorrem durante o "rescaldo", utilizando isso a seu favor (Stark & Fontaine, 2015).

À medida que as avaliações são recolhidas, as organizações precisam de uma maneira de analisá-las e gerar relatórios para as métricas que suportam[136]. As organizações precisam de reconhecer que, com o tempo, deverão alterar as suas medidas e métricas, porque embora as métricas de alto nível permaneçam as mesmas, as métricas de baixo nível precisam mudar ao longo do tempo, à medida que a postura de segurança se transforma (Black, *et. al* 2008).

Assim, esta iniciativa, através de *framework e workflows*, pretende lançar um "programa de cubicagem de segurança informática" com foco no alinhamento de medidas técnicas, determinação do efeito nos objetivos organizacionais, e apoio a tomada de decisões pelas administrações das empresas. Não só para efeitos de seguro informático e não apenas sobre a transferência de riscos, mas também com vantagens noutros aspetos empresariais, tanto para seguradoras enquanto salvaguarda, como para as empresas enquanto tomada de decisão mais consciente, consiste num trabalho preliminar, para entender possíveis desvantagens, falhas e outros alertas sobre a cibersegurança de uma empresa (NIST, 2017, a).

[136] Essa discussão, incluindo o desejo de ter melhores informações e ferramentas para avaliar a eficácia das estratégias e ações de segurança informática reflete a questão mais ampla da mensuração deste tipo de risco. Este é um tópico subdesenvolvido, no qual não há uma taxonomia padrão para termos como "medição" e "métrica", pelo que o desenvolvimento de formas confiáveis de medir o risco constitui um grande avanço e contributo para a segurança informática (NIST, 2017, a).

6. Conclusões

Através do presente estudo e principais resultados obtidos, conclui-se que os mesmos foram proveitosos, enriquecedores e promissores. Acredita-se que, a aplicação prática da framework construída permita retirar várias conclusões interessantes sobre o mercado (empresas) e para o mercado (seguradoras). Também se constata que, a dificuldade inerente a uma conceção deste tipo de modelos de risco é proporcional aos objetivos que se pretende atingir, riscos que se quer mensurar e ambição associada a este tipo de seguro.

Primariamente, foi possível constatar que o seguro informático é uma ferramenta importante para a segurança da Internet por alinhar incentivos para as seguradoras e por levar as organizações a administrarem os riscos corretamente, o que gera um mercado de cibersegurança que resulta em vantagens para o bem-estar social. Da mesma forma, veio a comprovar-se que, *frameworks* de risco complementares à triagem e pré avaliação por parte de uma seguradora, se constituem como uma mais valia e instrumento fundamental para a análise de riscos de forma bilateral, polivalente e detalhada.

A indústria seguradora informática tem um papel crucial em criar um espírito de sensibilização e formas de lidar com os riscos informáticos, dado a ameaça dependente da estrutura e a falta de informação, se constituírem como as principais dificuldades em modelar o risco informático. Constatou-se que, devem ser estruturados mais *frameworks* de análise de risco e também criadas bases de dados, com o correto acompanhamento de estrutura legal, para dar azo a uma *pool* de seguros informáticos para, por sua vez, ajudar a completar as falhas dos portefólios (existentes até à data) das seguradoras neste âmbito.

Segundo Tom Bolt - Lloyd’s Insurance (2017) - e (Jain,2017), a indústria de seguros informáticos tem vindo a revelar uma inovação real e demonstra a capacidade das seguradoras em desenvolverem apólices para cobrir riscos modernos e complexos. Devido à crescente importância desta classe de risco, os dados de exposição

padronizados são críticos para níveis mais altos de cobertura de seguro e melhor modelação do risco. Futuramente, haverá uma exposição informática que aumentará drasticamente, e onde, do lado da demanda haverá uma pobre consciência do risco, uma cobertura limitada e uma redação de apólices inconsistente por parte das seguradoras, e, do lado da oferta, verificar-se-á uma falta de compreensão das exposições/incertezas ao risco de acumulação, e, uma paisagem de risco em rápida evolução.

Em termos de questões legais paralelas a esta temática, constata-se que é a não regulamentação da matéria que permite o aumento do cibercrime, pelo que urge a elaboração de normas penais de carácter mais abrangente, não punindo somente condutas específicas. Não imperará a conceção de leis rígidas e de amplitude limitada, mas sim leis que criem uma possibilidade jurídica além-fronteiras.

No atual quadro legal português, existem algumas normas penais para incriminar condutas que se associam à disseminação da criminalidade informática. Contudo, sendo este um tipo de crime que existe muito por consequência, é fulcral que sejam suprimidos os vazios normativos ainda existentes em relação ao mesmo. Tal, deve ser feito de forma técnica e antecipatória, dada a extrema mutabilidade do mundo informático evitando-se assim excessos legislativos prejudiciais a uma boa regulamentação do tema.

Não obstante, importa relevar que, o tempo virtual se move rapidamente, enquanto os hábitos e normas humanas, bem como as práticas estatais, mudam muito mais lentamente. Para além de acordos bilaterais entre as principais potências mundiais, julga-se pertinente que, relativamente a certas normas de segurança para a Iot, o sector privado[137] como as companhias de seguros e partes interessadas (outras empresas de tecido empresarial das PME's e não só), devam assumir a liderança no

[137] "Uma vez que a maioria das redes e dos sistemas de informação são explorados pelo setor privado, a cooperação entre o setor público e setor privado é essencial. Os operadores de serviços essenciais e os prestadores de serviços digitais deverão ser incentivados a criar os seus próprios mecanismos de cooperação informal para garantir a segurança das redes e dos SI" – Consideração retirada da Diretiva (UE) 2016/1148.

desenvolvimento de códigos de conduta. Também as disposições constantes no RGPD vêm reforçar essa necessidade.

Hoje, um potencial ataque informático implica vários tipos diferentes de cobertura de seguro - dependendo de fatores como o tipo de ataque, a extensão, se houver, da perda de dados, o relacionamento das partes, a natureza dos dados envolvidos, o tipo de apólice em questão e, se ocorrer por responsabilidade de terceiros, quais as alegações e o tipo de danos em questão. Os danos causados por ataques informáticos são tão multifacetados que não há distribuição normal de resultados para avaliar as probabilidades de eventos e impactos futuros. A única hipótese, para já, será iniciar um percurso analítico com base no tipo de *frameworks* como a sugerida.

Secundariamente, no que respeita ao horizonte da gestão de riscos, este precisa de ser estendido muito além dos seus perímetros atuais, para todas as agregações de risco informático e especialmente para contratos terceirizados, cadeias de fornecimento e infraestrutura *upstream*. Foi igualmente verificado que, uma atuação na perceção do risco, implica não só conduzir mais pesquisas do lado da procura, analisar a segurabilidade e formas de a melhorar (especialmente pesquisa empírica, por exemplo, dados e análise de cenário), como também analisar a gestão de riscos informáticos (mitigação versus seguro) e quanto capital será necessário para cobrir os mesmos (cálculos para valor em risco).

O fato de a proteção total contra-ataques informáticos ser inatingível, fortalece o papel que o seguro pode desempenhar na remoção do risco mínimo e no aumento da resiliência geral da sociedade. No entanto, um bom funcionamento de mercado requer um entendimento da exposição ao risco que é, entre outros, um pré-requisito para uma estrutura adequada de gestão de riscos. A comunidade académica deve fazer parte do diálogo global sobre como prevenir este risco e como promover o seguro informático, a fim de fornecer o seu ponto de vista, e estabelecer um ponto crítico em relação àquilo, que certamente, será alvo de discussões futuras nas agendas e fóruns nacionais/internacionais.

Enquanto fruto da presente investigação, veio também a verificar-se que, as organizações são relutantes em divulgar informações sobre as suas vulnerabilidades e incidentes de risco informático, e que o agrupamento de informações permitirá a análise de tendências dos tipos de ataques e perdas, que por sua vez auxiliará as empresas a supervisionarem melhor a iminência do risco informático. "A perspetiva económica para a segurança da informação no geral, e a ideia do seguro contra riscos informáticos em particular, são abordagens promissoras para identificar e enfrentar as atuais questões de segurança, levando a uma infraestrutura de comunicação confiável para a sociedade da informação" (Böhme, 2005) e (Kitching *et. al*, 2014). As empresas devem, assim, ser mais permeáveis e contributivas na manutenção do equilíbrio do princípio liberdade-segurança, no que respeita a esta fragilidade.

Paralelamente, reforça-se que o modelo de fraude e ataques informáticos se acomodaram na rede com uma infinidade de técnicas distintas e polivalentes. Assim, neste registo, as manifestações fraudulentas são peculiares e muitas delas não conseguem ser processadas do ponto de vista jurídico, recorrendo-se a crimes como fraude, furto, acesso ilegítimo e outros. A escassa adaptação do meio ambiente, as circunstâncias em que manobram os criminosos, bem como a perceção limitada do risco, contribuíram para o impulsionar do fenómeno. Aqui, deve ter-se em atenção que, determinados incidentes não deverão ser categorizados como fraude informática (enquanto vetor do ataque/motivo do sinistro), mas sim como potencial fraude a seguradoras (burla de seguro enquanto objetivo) no âmbito dos seguros informáticos.

Apesar da segurança e transferência de riscos para as seguradoras, estas perturbações, irão sempre verificar-se (ainda que pontualmente) e serão de tal frequência e intensidade que a maioria das organizações terá de passar por elas. A principal esperança para as empresas é, portanto: a) a resiliência; b) a capacidade de recuperação de interrupções, tornando-as tão curtas e limitadas quanto possível; e c) a aplicação *in situ* de *frameworks* como a desenhada. Estas três subcategorias de recomendações, não só tornam a organização mais capaz de superar os impactos informáticos, mas à medida que são implementadas, elas atuam como amortecedores sistémicos, reduzindo potencialmente a magnitude sinistros deste tipo.

A framework criada, para aplicar num seguro informático, enquanto ferramenta de análise de risco (e simultaneamente contra o cibercrime) contempla uma dupla análise, multifacetada com várias finalidades em comum e que se intersetam. Como exemplo prático, uma empresa ao se submeter a este tipo de análise de risco detalhada, fornecendo este tipo de informações e ponderando com razoabilidade todos os aspetos técnicos, operacionais, de rede (e outros exemplos colocados diretamente em questionário, por exemplo), ficará com uma melhor noção, técnica e de risco, sobre a sua própria organização. Fica com um conhecimento próprio vantajoso, que servirá tanto para canalizar auditorias específicas, solicitar certificações em certos setores, realizar um seguro informático direcionado e objetivo quanto às pretensões de coberturas, e, fazer um upgrade na segurança informática no geral.

Neste seguimento, realça-se a importância de um acompanhamento técnico e direcionado por peritos que conduzam uma triagem tendo por base técnicas de *intelligence*, perícias técnicas entre outras, para todas as empresas que queiram submeter um seguro informático, mas também para as seguradoras em particular. A capacidade dos peritos informáticos deve ser valorizada e aproveitada enquanto especialistas em segurança de TI, o que oferecerá uma ampla gama de perspetivas sobre o assunto. Isto ajudará as seguradoras a reforçar a sua própria resiliência ao risco informático, mas também a desenvolver soluções de seguros para clientes, respetiva avaliação e orçamentação do risco mais célere e eficaz.

Apurou-se ainda que, o melhor tipo de modelos para o efeito são aqueles que contemplam métricas relacionadas com o risco, com a segurança informática e que, de forma tão detalhada quanto possível, sejam capazes de definir, qualitativamente, os principais riscos e setores de uma empresa mais frágeis, e, por outro lado, consigam, quantitativamente, chegar a um valor aproximado da importância que as informações, ativos e outros bens intangíveis têm na esfera empresarial em análise. Por extrapolação, inferência e dedução, tais valores em risco são estimados com base nas perdas ou prejuízos em que a empresa incorreria na eventualidade de ver determinado tipo de dados, informações, redes e equipamentos, comprometidos.

O resultado atingido consagra-se como sendo uma framework sólida, que necessitará obviamente de certos ajustes consoante testes e estudos de caso que sejam realizados. O maior obstáculo é construir uma framework base direcionada e focada no que se pretende, pois a partir do momento que exista uma rampa de lançamento no processo de elaboração de seguro informático, será intuitiva uma construção de mapas e conexões com outras frameworks pertinentes, para uma análise de risco, em dimensão macro e também pormenorizada.

Por último, ficou patente que as seguradoras lidam com um grau considerável de incertezas, mas, esta problemática não pode ser comparável com os seguros até aqui conhecidos. Atendendo à alta incerteza, pela natureza do risco, as seguradoras não devem confiar muito em modelos estatísticos, mas devem estabelecer sim limites baixos de cobertura e estipular exclusões estritas nas suas apólices informáticas. A melhor informação para qualquer tipo de modelação, advém de reclamações de sinistros deste tipo. Também é um risco que deve ser analisado do ponto de vista técnico e não estatístico, pela pobre qualidade dos dados. Por isto, existem limitações à cabal compreensão do funcionamento deste tipo de modelos de risco e ferramentas complementares.

Também foi apurado que, em futuras investigações[138], será pertinente aplicar métricas mais detalhadas, e se possível, moldar questionários e frameworks diretamente para departamentos de TI ou informática, no sentido de apurar possíveis riscos críticos e compreender os ativos mais valiosos e debilitados de uma empresa. Assim, seria mais simples identificar as principais vulnerabilidades de uma empresa, reforçando o plano de seguro nesse sentido. Contudo, ainda será uma batalha e avanço com progressão compassada, atendendo a questões éticas, de segurança e de permeabilidade de acessos, relativamente a esferas mais sensíveis de negócios e interesses comerciais.

[138] Para a presente taxonomia e qualquer outro modelo, serão necessárias revisões futuras para adaptação à constante mudança do cenário virtual. Este tipo de modelos*/frameworks/workflows* carecem de ser validados através de trabalho de campo, com organizações em níveis variados (quer na tolerância a riscos como na conformidade regulatória, entre outros) (Cebula, & Young, 2010).

Futuras investigações podem concentrar-se, também, em aplicações individuais do estudo ou avaliar o risco pré-apólice, sob a perspetiva de um cliente em concreto. Um tema atual seria examinar os efeitos pós-seguros num ambiente de clientes, ou seja, como funcionaria a ativação do seguro após sinistro informático – testar a aplicabilidade prática da *framework*– mais na esfera da *incident response*. Poderão ainda ser feitas prospeções de mercado relativas a smartphones, sistemas Android, no âmbito das Iot e relacionados[139].

Termina-se com uma reflexão, recordando a relevante teoria de Nassim Taleb, onde, na sua obra "A Lógica do Cisne Negro", nos explica o impacto do altamente improvável, demonstrando como estamos constantemente à mercê do inesperado, o que obviamente se cruza com os objetivos e pretensões da presente dissertação. O risco informático é imprevisível, ocasiona resultados impactantes e, após a sua ocorrência, inventaremos um meio de torná-lo menos aleatório e mais explicável. "O mundo em que vivemos tem um número crescente de ciclos de *feedback*, fazendo com que os eventos sejam a causa de mais eventos, gerando assim bolas de neve arbitrárias e imprevisíveis, com efeitos que prevalecem em todo o planeta". Neste caso, em toda a organização/empresa. É por isso que se acredita que esta proposta se constitui como uma importante solução, contribuindo para a segurança efetiva dos sistemas de informações, transparência das relações seguradores/segurados e consequente incremento da segurança dos negócios.

[139] Aplicação em dimensão micro dos seguros informáticos.

7. Referências Bibliográficas

ARTIGOS CIENTÍFICOS

ACS, (2016). Cybersecurity – Threats, Challenges and Opportunities. *Australian Computer Society, 50 Carrigton Street, Sydney*. November, 2016. Disponível em www.acs.org.au.

Adeleke, I. et al. (2011). Cyber Risk Exposure and Prospects for Cyber Insurance. *Department of Actuarial Science and Insurance, University of Lagos, Nigeria , IAU. Int. J. Manag. Bus. Res., 1 (4), 221-230,* Autumn 2011.

Allianz, (2017). Allianz Cyber Protect - Cyber Insurance. *A comprehensive cyber insurance provided internationally and tailored to your company´s risk profile*. Disponível em http://www.agcs.allianz.com/services/financial-lines/cyber-insurance/.

Amaral, N. F (2014). Geolocalização em atividades físicas: Aplicação e Expetativas. *Instituto Superior de Engenharia do Porto*. Dissertação no âmbito do Mestrado em Engenharia Informática. Porto.

Anderson, R. (2013). Insurance Coverage for Cyber Attacks. Legal Insight – *The Insurance Coverage Laz Bulletin, Vol. 12, No, 5, Part Two of a Two-Part Article.* K&L Gates, June 2013.

Anderson, R. (2014). Cyber-Attacks: Insurance Coverage for Cyber Risks and Realities- *K&L Gates,* 25 June, 2014. U.K.

Arien, G. M. (2003). Los Contratos Informaticos. *Saberes – Revista de estúdios jurídicos, económicos y sociales,* Volumen 1. Universidade Alfonso X El Sabio. Villanueva de la Cañadá.

Axa, (2017). Sector de la informática. *Empresa – Axa Seguros. Garantias y Ventajas.* Disponível em: https://www.axa.es/seguros-empresas/sector-informatica-garantias#link2.

Azevedo, A. H. F (2016). Burlas Informáticas: Modos de Manifestação. *Universidade do Minho, Escola de Direito*. Dissertação no âmbito do Mestrado em Direito e Informática.

Bacelar, J.G (2017). Estudos de Direito e Segurança, vol.II, *ISBN 978-972-40-5836-8,* Almedina, Coimbra. Fevereiro, 2017.

Bacelar, J. G. (2018). Manual de Direito Constitucional, vol. I – *Teoria do Direito Constitucional, 6ª edição, ISBN 978-972-40-6795-7,* Almedina, Coimbra.

Bandyopadhyay, T. *et al*. (2009). Why IT Managers Don't go for Cyber-Insurance Products. *Communications of the Association for Computing Machinery, Vol. 52, nº. 11*. November 2009.

Bernal, J. S, (2009). El bien jurídico protegido en el delito de estafa informática. *Universidad de Salamanca, CT 1 (2009) pp. 105-121*. Espanha.

Biener, C. et al. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Institute of Insurance Economics - University of St. Gallen*, January, 2015.

Black, P. *et. al* (2008). Cyber Security Metrics and Measures. *National Institute of Standards and Technology - Wiley Handbook of Science and Technology for Homeland Security, John Wiley & Sons, Inc.* Gaithersburg, Maryland.

Böhme, R. (2005). Cyber-Insurance Revisited. *Workshop on the Economics of Information Security (WEIS)* – Kennedy School of Government, Cambridge, MA, USA.

Bolot, J & Lelarge, M. (2008). Cyber Insurance as an Incentive for Internet Security. *WEIS 20081, Seventh Workshop on the Economics of Information Security,* Hanover NH (USA), June 25-28, 2008.

Bonet, A. E. (2012). Risk Management Drives – Credibility and Transparency. *Gerencia de Riesgos y Seguros Nº112 – 2012*.

Boyens, J. *et al.(*2015). Supply Chain Risk Management Pratices for Federal Information Systems and Organizations. *NIST Special Publication 800-161. Computer Security – US Department of Commerce.* Washington, April 2015. Disponível em http://dx.doi.org/10.6028/NIST.SP.800-161.

Bravo, R *et al.*, (2012). Proteção do Ciberespaço: Visão Analítica, *Edições Salamandra, (ISBN 978-972-689-247-2), pp.163 a 176*. Lisboa, 2012.

Bressler, M. (2014). Protecting your company's intelectual property assets from cyber-espionage. *Journal of Legal, Ethical and Regulatory Issues,* Volume 17, (2).

BritInsurance, (2017). Cyber Attack Insurance. United Kingdom. Disponível em http://www.britinsurance.com/brit-global-specialty/global-cyber-privacy-technology.

Brown, H. (2005). Espionage, theft and greed restate: the need for protection. Disponível em http://documentslide.com/documents/espionage-theft-and-greed-restate-the-need-for-protection.html, acedido em 21 de agosto de 2018.

Cazelatto, C. C & Moreno, M. H (2016). Da Sociedade da Informação frente ao acesso à Internet como um Direito Fundamental de personalidade. *Revista de Direito, Governança e Novas Tecnologias*, e-ISSN: 2526-0049, Brasília, v. 2 , n. 1 , p. 92 - 112 , Jan/Jun. 2016.

Cebula, J & Young, L. (2010). A Taxonomy of Operational Cyber Security Risks. *Software Engineering Institute - CMU/SEI-2010-TN-028, Cert Program,* University Carnegie Mellon. Pittsburgh.

Cordeiro, A. M. *et al* (2017). FINTECH: Desafios da Tecnologia Financeira, *Edições Almedina S.A ISBN 978-972-40-7180-0.* 25 Março de 2017, Lisboa.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons,* Volume 48, pp. 233-240.

Culp, S. & Thompson, C., (2016). The Convergence of Operational Risk and Cyber Security. Accenture, Chartis.

Denzin, N. K , (1970). The Research Act. A Theoretical Introduction to Sociological Methods. *AlzineTransaction – A Division of Transaction Publishers. ISBN: 978-0-202-36248-9.* New Brunswick and London, 2009.

Dias, V. M (2012). A Problemática da Investigação do Cibercrime. *DataVenia, Revista Jurídica Digital, ISSN 2182-6242, Ano 1 Nº01* Junho-Dezembro 2012.

Dobie, G. (2015). A Guide to CyberRisk – Managing the Impact of Increasing Interconnectivity. *Allianz Global Corporate & Speciality SE, Germany* – September 2015.

Drouin, D. (2004). Cyber Risk Insurance – A Discourse and Preparatory Guide. *GIAC Security Essentials Certification,* SANS Institute, InfoSec Reading Room. Swansea, U.K.

Eling, M. & Schnell, W (2016). Ten Key Questions on Cyber Risk and Cyber Risk Insurance, *International Association for the Study of Insurance Economics, Geneva Association*. November, 2016.

Eling, M. & Schnell, W. (2016 a). Recent Research Developments Affecting Non-Life Insurance - *The CAS Risk Premium - Project 2016 Update*. *Institute of Insurance Economics,* University of St. Gallen, Switzerland.

Eling, M. & Wirfs, J. H. (2015). Modelling and Management of Cyber Risk. *Institute of Insurance Economics - University of St. Gallen*, Switzerland.

ENISA, (2012). Incentives and barriers of the cyber insurance market in Europe. *Resilience and CIIP Program, European Network and Information Security Agency (ENISA),* P.O. Box 1309, 71001 Heraklion, Greece – June 2012.

ENISA, (2016). Cyber Insurance: Recent Advances, Good Pratices and Challenges. *ISBN 978-92-9204-178-6. European Union Agency for Network and Information Security Science and Technology Park of Crete (ITE),* 700 13, Heraklion, Greece – November 2016.

Fernández. G. (2007). La Transferencia de riesgos. Actuarios - *Universidad Carlos III, Madrid.* Julio, 2007.

Fiães Fernandes, L. (2005). As "Novas" Ameaças como Instrumento de Mutação do Conceito "Segurança", em M.M.G. Valente (Ed.), *I Colóquio de Segurança Inter*na. (pp. 123-152). Coimbra: Almedina.

Fitzpatrick, W. & Dilullo, S. (2015). Cyber Espionage and the S.P.I.E.S. Taxonomy. CF, Volume 13 (2).

Fraguio, M. P. D. & Macías, M. I. C (2011). Gerencia de Riesgos Sostenibles y Responsabilidad Social Empresarial en la Entidad Aseguradora. *Instituto de Ciencias del Seguro – Fundación Mapfre* 978-84-9844-264-9. Madrid.

Garcia, F. P. (2006). As Ameaças Transnacionais e a Segurança dos Estados, Subsídios para o seu Estudo, *in Revista Negócios Estrangeiros n.º 9.1.*, (Lisboa: Instituto Diplomático, Ministério dos Negócios Estrangeiros, 2006), p. 340.

Gomes, H. D (2017). "Comunicações Eletrónicas e Segurança Empresarial", *em Estudos de Direito e Segurança (coord. de Bacelar Gouveia),* II vol., pp. 157-167, *ISBN 978-972-40-5836-8,* Almedina, Coimbra. Fevereiro, 2017.

Gómez, E. C. F. e Espinosa, H.A. C (2014). Cómo responder a un Delito Informático. *Revista Ciencia UNEMI, Nº11,* Junio 2014, pp. 43-50 ISSN: 1390-4272. Equador.

González, L. O. M. (2017). Contratos informáticos: Riesgos y Seguros. *Universidad Autonoma de Baja California, Facultad de Derecho Mexicali.*

Gordon, L. et al. (2003). A framework for using insurance for cyber-risk management. *Communications of the Association for Computing Machinery, Vol. 46, nº. 3.* March 2003.

Gubbi, J. *et al* (2013). Internet of Things (Iot) : A vision, architectural elements, and future diretions. *Future Generation Computer Systems 29, 1645-1660*. Elsevier, University of Melbourne - Australia.

Healey, J. (2014). Risk Nexus – Beyond data breaches: global interconnections of cyber risk. *Zurich Insurance Company Ltd and Atlantic Council of the United States,* April 2014.

Hiscox, 2017. Seguro para profesionales en Informática y Tecnología. *Hiscox* Espanha. Disponível em : http://www.hiscox.es/hiscox-rc-tic

Inácio, A. (2017). Segurança nos negócios – Conhece os seus prestadores de serviços? *in Vida Económica, Grupo Editorial*. Publicado em 2017.

Inácio, A. (2017a). Segurança nos negócios – Regulamento Europeu de Proteção de dados – Acha que está preparado? *in Vida Económica, Grupo Editorial*. Publicado em 2017.

Iruena,(2015). Seguro de Riesgos Informáticos, Cibernéticos o de Internet - *Iruena Global Correduria de Seguros*. Madrid. Disponível em : www.iruena.com / http://www.iruena.com/seguros-para-empresas/seguro-riesgos-informaticos-ciberneticos/.

ITSO (2007). Virginia Tech Guide for Cyber Security Incident Response – IT Security Office.

J. Marine, F. (1999). The Threats posed by Transnational Crimes and Organized Crime Groups. *Work Product of the 108th International Seminar, Resource Material Series No. 54.* UNAFEI: United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders. Nº54 (1999) p. 25-53.

Jain, A. (2017). Modelling Cyber Risk. *Air WorldWide.*

Jones, A. & Jones, A. (2008). Industrial espionage in a hi-tech world. *Computer Fraud & Security.*

Kesan, J. & Zhang, L. (2016). Security Metrics for Cyber Insurance. *Critical Infrastructure Resilience Institute.* A Homeland Security Center of Excellence. Illinois.

Kesan, J. et al (2004). Cyberinsurance as a Market Based Solution to the problem of CyberSecurity – A case study. *University of Illinois at Urbana-Champaign.*

Kitching, N. *et. Al* (2014). Cyber Resilience – The cyber risk challenge and the role of insurance. *CRO Forum*, December 2014.

Krickhahn, J. (2015) - Practice Leader Cyber & Fidelity at AGCS Financial Lines Central & Eastern Europe. Disponível em www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2015_EN.pdf.

Lee, K. (2015). The Internet of Things (Iot): Applications, investments, and challenges for enterprises. *Business Horizons, Kelley School of Business* – Indiana University.

Lima, A. S, (2017). Cibercrimes e a sua configuração no plano jurídico nacional e internacional. *Universidade Federal do Maranhão, Centro de Ciências Sociais, Curso de Direito*. São Luís.

Lloyd's, (2016). Facing the cyber risk challenge – *A report by Lloyd's.* 20 September 2016.

Lloyd's, (2017 a). Facing the cyber risk challenge – *Key highlights (for Spain, Sweden, UK and Germany)* Disponível em: lloyds.com/cyber.

Lloyd's, (2017). Why buy cyber insurance at Lloyd's? *Lloyd's of London*. Disponível em : https://www.lloyds.com/lloyds/about-us/what-do-we-insure/what-lloyds-insures/cyber/why-cyber-insurance.

Majuca, R. *et al.* (2006). The Evolution of Cyber Insurance- *University of Illinois at Urbana-Champaign.* February, 2006.

MAPFRE, (2010). Revista Gerencia de Riesgos y Seguros Nº107-2010. *Fundación Mapfre – Instituto de Ciencias del Seguros,* Madrid.

Masseno, M.D, (2014). Direito Fraterno Humanista e Globalização Jurídica e Constitucional – Desafios Filosóficos e Práticos: Liberdade e Segurança na Sociedade em Rede. Outubro de 2014, Porto.

Masseno, M.D. (2011). O Direito perante os riscos tecnológicos na EU – Segurança na Internet, no meio ambiente e nos alimentos. *Instituto Jurídico Interdisciplinar da Faculdade de Direito da Universidade do Porto.* Novembro, 2011.

Masseno, M.D. (2011, a). As Leis Portuguesas do Cibercrime – um esboço esquemático. *Jornadas Luso-Brasileiras, Cibercriminalidade e Segurança Informática*. 22 Junho de 2011.

Masseno, M.D. (2015). On the limits of cybercrime investigation – a brief European approach. *Workshop on Eletronic Discovery and Digital Evidence.* Universidade do Minho, 2015.

McCulloch, J. & Pickering, S., (2009). Pre-Crime and Counter-Terrorism – Imaginin Future Crime in the 'War on Terror'. *Center for Crime and Justice Studies (ISTD)Brit. J. Criminol.* (2009) vol. 49, pp. 628-645. Oxford University.

Molitor, H. & Velazquez, V. (2017). Breve Panorama Sobre a Legislação Aplicada nos Crimes Eletrónicos. *Revista de Direito, Governança e Novas Tecnologias.* e-*ISSN: 2526-0049*, Maranhão, v. 3, n. 2, p. 81 – 96, Jul/Dez. 2017.

Mueller, R. S., (2012). Combating Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies. *RSA Cyber Security Conference - Director*; *Federal Bureau* of *Investigation -San Francisco,* CA*;* March 01, 2012.

Mukhopadhyay, A. *et al*. (2005). Insurance for Cyber-Risk: A Utility Model. *Decision, Vol. 32, No.1, Indian Institute of Management Calcutta.* January - June, 2005.

Mukhopadhyay, A. *et al.* (2013). Cyber Risk decision models: To insure IT or not? *Decision Support Systems, Elsevier (2013),* Disponível em: http://dx.doi.org/10.1016/j.dss.2013.04.004.

Muravska, J. (2013). Cyber War Will Not Take Place. Disponível em: *http://blogs.lse.ac.uk/lsereviewofbooks/2013/06/17/book-review-cyber-war-will-not-take-place/,* acedido em 11 de março de 2018.

Nelson, N. (2016). How companies achieve balance between techonology enabled innovation and cyber-security. *Working Paper CISL, Massachusetts Institute of Techonology* # 2016-01.

Neto, J. A. M (2003). Crimes informáticos uma abordagem dinâmica ao direito penal informático. *Pensar, Fortaleza, v. 8, n. 8*, p. 39-54, fev. 2003.

NIST, (2017). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology - Draft Version 1.1. NIST* January 10, 2017.

NIST, (2017, a). Roadmap for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology - Draft Version 1.1*. NIST December 5, 2017.

Noonan, M. (2011). Cyber Insurance. *MARSH, Managing Principal, New Zealand Marsh Ltd* |, Christchurch, New Zealand.

Ocidental, (2015). Seguro Multirrisco Equipamento Eletrónico Informático – Condições Gerais e Especiais da Apólice. *Ocidental - Companhia Portuguesa de Seguros S.A*, Junho 2015.

Ögüt, H. *et al*. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Rik, Imperfect Ability to Prove Loss, and Observability of Self-Protetion. *Society for Risk Analysis, Risk Analysis, Vol. 31, No. 3, 2011. 0272-4332/11/0100-0497$22.00/1 C.*

Pazmiño, J. *et al* (2017). Big Data Analytics: a contribution in the business solution. *Pro Sciences: Revista de Produccion , Ciencias e Investigacion, ISSN: 2588-1000, Vol. 1, N 2,* September 2017, PP. 21-25. Universidad Técnica de Babahoyo.

Pazmiño, J. *et al* (2017a). La seguridade informática y su impacto en las conexiones del estándar. *Pro Sciences: Revista de Produccion , Ciencias e Investigacion, ISSN: 2588-1000,* Vol. 1, N 4, Noviembre 2017, PP. 3-6. Universidad Técnica de Babahoyo.

Pereira, M. M. M (2013). O Custo da Fraude no Sinistro Ramo Automóvel. Estudo de Caso – Garantia Seguros. *Instituto Superior de Ciências Económicas e Empresariais – Licenciatura em Contabilidade e Administração - Ramo Auditoria.* Lisboa.

Pereira, R. (2017). "Crime Económico – Perspetivas Dogmáticas e Desafios Político-Criminais", *em Estudos de Direito e Segurança (org. de Bacelar Gouveia),* I vol., pp. 357-371, *ISBN 978-972-40-5822-1,* Almedina, Coimbra. Fevereiro, 2017.

Pereira, R. (2017, a). "A Segurança na Constituição", *em Estudos de Direito e Segurança (coord. de Bacelar Gouveia),* II vol., pp. 409-423, *ISBN 978-972-40-5836-8,* Almedina, Coimbra. Fevereiro, 2017.

Power, R. & Forte, D. (2007). Information age espionage, debriefing a real-world, top-class cyber sleuth. *Computer Fraud & Security.*

Ralph, O. (2017). Insurance Correspondent - Financial Times. *Insurer Beazley Group*, May, 2017).

Rid, T. (2012). Cyber War Will Not Take Place. *The journal of strategic studies*. Volume 35 (1) pp.5-32.

Rogerson, M. & Pease, K. (2004). Privacy, Identity and Crime Prevention. *Document Review in Cyber Trust & Crime Prevention Projet.* University of Huddersfield, UK.

San José-Marti, I. C (2013). Proceso de Gestión de Riesgos y Seguros en Las Empresas. *Casares, Asesoría Actuarial y del Riesgos, S.I.* Madrid.

Santiago, C. (2016). Risco informático torna-se um risco corporativo. Disponível em: *https://www.marsh.com/br/insights/research/risco-cibernetico-torna-se-um-risco-corporativo.html,* acedido em 29 de Março de 2018.

Santos, A. F. C (2015). O Cibercrime: Desafios e Respostas do Direito. *Universidade Autónoma de Lisboa, Departamento de Direito.* Dissertação de Mestrado em Direito - Ciências Jurídicas. Lisboa.

Santos, L. (2017). "Contributos para uma melhor Governação da Cibersegurança em Portugal", *em Estudos de Direito e Segurança (coord. de Bacelar Gouveia),* II vol., pp. 217-307, *ISBN 978-972-40-5836-8,* Almedina, Coimbra. Fevereiro, 2017.

Santos, L. & Guedes, A. M, (2015). Breves reflexões sobre Poder e Ciberespaço, *RDeS – Revista de Direito e Segurança, n.° 6 (julho / dezembro de 2015): 189-209.* Lisboa.

Shackelford, S. (2012). Should Your Firm Invest in Cyber Risk Insurance. *Center for Applied Cybersecurity Research - Kelley School of Business,* Indiana University, Bloomington.

Skinner, C. (2014). An International Law Response to Economic Cyber Espionage. *Connecticut Law Review*. Volume 46 (4).

Stark, R. J. & Fontaine, R. D (2015). CyberInsurance: A Pragmatic Approach to a Growing Necessity. *CyberSecurity Docket - Docket Media LLC – Global CyberSecurity and Incident Response Report.* April, 10, 2015.

Talbot, D. (2015). Cyber-Espionage Nightmare. *Mit Technology, Volume 118* (4).

Tenzer, S. M & Sena, L. (2004). Introducción a Riesgo Informático. FCEA – Cátedra Introducción a la Computanción. Espanha.

Teruelo, J. G. F (2007). Respuesta Penal Frente a Fraudes cometidos en Internet: Estafa, Estafa Informática y los Nudos de la Red. *Revista de Derecho Penal y Criminologia. 2ª Época, n19, pp. 217-243.* Oviedo, Espanha.

Van Houtte, P. (1994). El Seguro de Responsabilidad Civil Profesional de los Informáticos. *Centro de Investigación de Informática y Derecho* (CRID). Belgica.

Veiga, P. & Dias, M (2010). A Internet e as novas dimensões legais. *As grandes redes do conhecimento, Revista JANUS 2011-2012, NET e-journal of International Relations,* Vol.1, nº1.

Verdelho, P. (2003) Cibercrime. *In Direito da Sociedade da Informação – Vol. IV, Associação Portuguesa do Direito Intelectual*. Coimbra Editora, 2003, pp. 348 -352.

Watkins, B. (2014). The Impact of Cyber Attacks on the Private Sector. *Association for International Affairs.*

FONTES INSTITUCIONAIS

Center for Strategic and International. The Economic Impact of Cybercrime and cyber espionage. Studies - CSIS (2013).

Comissão Europeia, *Comunicação da Comissão ao Conselho e ao Parlamento Europeu. Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade.* Consultado a 01 de abril de 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52012DC0140&from=PT.

European Comission, (2016). Different forms of cooperation between insurance companies and their respective impact on competition. *Studies on issues pertaining to the insurance production process with regard to the application of the Insurance Block Exemption Regulation (IBER). ISBN 978-92-79-61488-0.* Luxembourg: Publications Office of the European Union.

JURISPRUDÊNCIA E LEGISLAÇÃO

Carta dos Direitos Fundamentais da União Europeia, de 18 de dezembro de 2000, disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf (consultado em 25 de março de 2018).

Código Civil, 2017. DL n.º 47344/66, de 25 de Novembro – Procuradoria Geral Distrital de Lisboa.

Código Penal, 2015 – 5ª Edição. Almedina.

Constituição da República Portuguesa, 2012 – 2ª Edição. Quid Juris.

Convenção sobre o Cibercrime, de 23 de novembro de 2001, disponível em: https://rm.coe.int/16802fa428 (consultado em 01 de abril de 2018).

Decreto-Lei n.º 72/2008, de 16 de abril, disponível em: http://www.asf.com.pt/winlib/cgi/winlib.exe?skey=&pesq=2&doc=17177# (consultado em 24 de março de 2018).

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 06 de julho de 2016, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT (consultado em 3 de março de 2018).

Diretiva n.º 2009/138/CE, do Parlamento Europeu e do Conselho, de 25 de novembro, disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009L0138&from=pt (consultado em 3 de março de 2018).

Lei n.º 109/2009, de 15 de setembro, disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis (consultado em 25 de março de 2018).

Lei n.º 37/2008, de 06 de agosto, disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1004&tabela=leis (consultado em 24 de março de 2018).

Lei n.º 96/2017, de 23 de agosto, disponível em: https://dre.pt/application/conteudo/108041475 (consultado em 25 de março de 2018).

Lei nº. 144/2015, de 08 de setembro, disponível em: https://dre.pt/web/guest/pesquisa/-/search/70215248/details/maximized (consultado em 22 de janeiro de 2018).

Lei nº. 63/2011, de 14 de dezembro, disponível em: https://dre.pt/application/conteudo/145578 (consultado em 3 de março de 2018).

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de de 27 de abril de 2016, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT (consultado em 15 de agosto de 2018).

8. Anexos

8.1. ANEXO 1 – Conjunto de tabelas representativas da taxonomia do risco informático, principais ativos, tipos de cobertura e apólices

Tabela I *- Descriminação das principais categorias de risco informático.*

Category	Description	Elements
Subcategory 1: actions of people		
1.1 Inadvertent	unintentional actions taken without malicious or harmful intent	mistakes, errors, omissions
1.2 Deliberate	actions taken intentionally and with intent to do harm	fraud, sabotage, theft, and vandalism
1.3 Inaction	lack of action or failure to act in a given situation	lack of appropriate skills, knowledge, guidance, and availability of personnel to take action
Subcategory 2: systems and technology failures		
2.1 Hardware	risks traceable to failures in physical equipment	failure due to capacity, performance, maintenance, and obsolescence
2.2 Software	risks stemming from software assets of all types, including programs, applications, and operating systems	compatibility, configuration management, change control, security settings, coding practices, and testing
2.3 Systems	failures of integrated systems to perform as expected	design, specifications, integration, and complexity
Subcategory 3: failed internal processes		
3.1 Process design and/or execution	failures of processes to achieve their desired outcomes due to poor process design or execution	process flow, process documentation, roles and responsibilities, notifications and alerts, information flow, escalation of issues, service level agreements, and task hand-off
3.2 Process controls	inadequate controls on the operation of the process	status monitoring, metrics, periodic review, and process ownership
3.3 Supporting processes	failure of organizational supporting processes to deliver the appropriate resources	staffing, accounting, training and development, and procurement
Subcategory 4: external events		
4.1 Catastrophes	events, both natural and of human origin, over which the organization has no control and that can occur without notice	weather event, fire, flood, earthquake, unrest
4.2 Legal issues	risk arising from legal issues	regulatory compliance, legislation, and litigation
4.3 Business issues	risks arising from changes in the business environment of the organization	supplier failure, market conditions, and economic conditions
4.4 Service dependencies	risks arising from the organization's dependence on external parties	utilities, emergency services, fuel, and transportation

Legenda: Principais categorias de risco informático, distribuídas por quatro ativos fundamentais, organizadas em dimensões selecionadas para a *framework* de análise de risco, com a devida descrição e principais elementos, reunidos de forma sintética
Fonte: (Biener, 2015).

Tabela II *- Principais coberturas de seguro informático.*

Coverage	Cause of cyber loss	Insured losses
Panel A: Third Party		
Privacy Liability	- Disclosure of confidential information collected or handled by the firm or under its care, custody, or control (e.g., due to negligence, intentional acts, loss, theft by employees)	- Legal liability (also defense and claims expenses (fines), regulatory defense costs) - Vicarious liability (when control of information is outsourced) - Crisis control (e.g., cost of notifying stakeholders, investigations, forensic and public relations expenses)
Network Security Liability	- Unintentional insertion of computer viruses causing damage to a third party - Damage to systems of a third party resulting from unauthorized access of the insured - Disturbance of authorized access by clients - Misappropriation of intellectual property	- Cost resulting from reinstatement - Cost resulting from legal proceeding
Intellectual Property and Media breaches	- Breach of software, trademark and media exposures (libel, etc.)	- Legal liability (also defense and claims expenses (fines), regulatory defense costs)
Panel B: First Party		
Crisis Management	- All hostile attacks on information and technology assets	- Costs from specialized service provider to reinstate reputation - Cost for notification of stakeholders and continuous monitoring (e.g., credit card usage)
Business Interruption	- Denial-of-service attack - Hacking	- Cost resulting from reinstatement - Loss of profit
Data Asset Protection	- Information assets are changed, corrupted, or destroyed by a computer attack - Damage or destruction of other intangible assets (e.g., software applications)	- Cost resulting from reinstatement and replacement of data - Cost resulting from reinstatement and replacement of intellectual property (e.g., software)
Cyber Extortion	- Extortion to release or transfer information or technology assets such as sensitive data - Extortion to change, damage, or destroy information or technology assets - Extortion to disturb or disrupt services	- Cost of extortion payment - Cost related to avoid extortion (investigative costs)

Legenda: Descrição de coberturas principais com respetivas causas prováveis/comuns do ataque informático e respetivas perdas garantidas. Destacam-se entre coberturas de primeira e terceira parte, com as respetivas cláusulas assentes no tipo da causa do sinistro. Paralelamente, registam-se exemplos de prejuízos advindos e inerentes a cada uma das cláusulas/coberturas.
Fonte: (Biener, 2015) e (Eling & Wirfs 2015)

Tabela III *- Taxonomia de riscos operacionais.*

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disasters**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
1.2 Deliberate	2.1.4 Obsolescence	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2.1 Fraud	**2.2 Software**	3.1.5 Information flow	4.1.5 Unrest
1.2.2 Sabotage	2.2.1 Compatibility	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.3 Theft	2.2.2 Configuration management	3.1.7 Service level agreements	**4.2 Legal issues**
1.2.4 Vandalism	2.2.3 Change control	3.1.8 Task hand-off	4.2.1 Regulatory compliance
1.3 Inaction	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3.1 Skills	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.2 Knowledge	2.2.6 Testing	3.2.2 Metrics	**4.3 Business issues**
1.3.3 Guidance	**2.3 Systems**	3.2.3 Periodic review	4.3.1 Supplier failure
1.3.4 Availability	2.3.1 Design	3.2.4 Process ownership	4.3.2 Market conditions
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Economic conditions
	2.3.3 Integration	3.3.1 Staffing	**4.4 Service dependencies**
	2.3.4 Complexity	3.3.2 Funding	4.4.1 Utilities
		3.3.3 Training and development	4.4.2 Emergency services
		3.3.4 Procurement	4.4.3 Fuel
			4.4.4 Transportation

Legenda: Dimensões de risco informático selecionadas para incorporação na *framework* em análise. É possível verificar quais os ramos e características internas a cada uma delas.
Fonte: (Cebula & Young, 2010).

Tabela IV *- Exemplos de tipo de incidentes informáticos.*

Incident Type	Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a university network, system, application, data, or other resource.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.
Improper or Inappropriate Usage	When a person violates acceptable computing policies.
Suspected PII Breach	If an incident involves personally identifiable information (PII) a breach is reportable by being merely **Suspected**. (Suspected PII incidents can be resolved by confirmation of a non-PII determination.)
Suspected loss of Sensitive Information	An incident that involves a suspected loss of sensitive information (not PII) that occurred as a result of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) Use, where the cause or extent is not known.

Legenda: Resumo técnico de alguns tipos de ocorrências informáticas associados às respetivas causas e que retratam de que forma podem ocorrer falhas de segurança, por motivo tecnológico.
Fonte: (ITSO, 2007) – Incident Response Management: NASA Information Security Incident Management.

8.2. ANEXO 2 - Conjunto de tabelas que contemplam vários tipos e opções de escolha em seguros informáticos, com descriminação de coberturas contratadas e exclusões associadas

COVERAGE	Net Advantage Security	e-Comprehensive	Webnet Protection
First Party Coverages			
Destruction, disruption or theft of info assets	Y	Y	Y
Internet Business Interruption	Y	Y	Y
Cyberextortion	Y	Y	Y
Fraudulent electronic transfers	N	Y	N
Denial of service attack		Y	Y
Rehabilitation expenses		Y	Y
Third Party Coverages			
Internet Content	Y	Y	Y
Internet Security	Y	Y	Y
Defense Costs	Y	Y	Y

COVERAGE \ Net Advantage Product	1	2	3	4	5	6	7
Network Security Liability			Y	Y		Y	Y
Web Content Liability	Y	Y	Y	Y		Y	Y
Internet Professional Liability		Y		Y			Y
Network Business Interruption					Y	Y	Y
Information Asset Coverage					Y	Y	Y
Identity Theft			Y	Y	Y	Y	Y
Extra Expense					Y	Y	Y
Cyber-extortion			Y	Y	Y	Y	Y
Cyber-terrorism	Y	Y	Y	Y	Y	Y	Y
Criminal Reward Fund					Y	Y	Y
Crisis Communication Fund					Y	Y	Y
Punitive, Exemplary and Multiple Damages	Y	Y	Y	Y		Y	Y
Physical Theft of Data on Hardware/Firmware			Y	Y		Y	Y

EXCLUSIONS	Net Advantage Security	e-Comprehensive	Webnet Protection
Failure to back-up	Y	Y	Y
Failure to take reasonable steps to maintain and upgrade security	Y	Y	Y
Fraudulent, dishonest and criminal acts of insured	Y	Y	Y
Ordinary wear and tear of insured's info assets	Y	Y	Y
Claim arising out of liability to related parties	Y	Y	Y
OTHER RELEVANT PROVISIONS			
Retentions	Y	Y	Y
Liability Limits	Y	Y	Y
Criminal Reward Fund/Investigative Expenses Covered	Y		Y
Services by Information Risk Group to mitigate the impact of 1st party loss, covered		Y	
Representations Relied Upon	Y	Y	Y
Regular/Annual Surveys of Insured's Facilities	Y	Y	Y

Figura 1 *- Tipos de opções de seguros.*

Tipologias disponíveis de opções de escolha em seguros informáticos, com descriminação de coberturas contratadas e exclusões associadas. Respetivamente, tem-se: tabela sumária de apólices recentes de seguros informáticos; diferentes produtos de seguro informático consoante a diferente estratégia, e, exclusões associadas a apólices de seguro informático. ***Fonte:*** *(Majuca 2006).*

Option	Description
General Internet Crime Liability	Addresses the first- and third-party risks associated with e-business, the Internet, networks and informational assets. Limitations exist with this level of coverage. It is key to review your business activities to ensure appropriate coverage.
Property	Protection against damage to hard assets caused via the internet, machinery taken down, or equipment programmed to operate erratically. Typically, this policy does not acknowledge "data" as property.
Errors and Omissions (see Professional Liability)	E&O liability protects your organization from claims if your client holds you responsible for programming errors, software performance, or the failure of your work to perform as promised in your contract.
Professional Liability (see Errors & Omissions)	Provides protection against claims that the policyholder becomes legally obligated to pay as a result of an error or omission in his/her professional work. Also known as Errors and Omissions insurance, this type of professional liability insurance is critical to your business. E&O insurance responds to claims of professional liability in the delivery of your technical services.
Directors and Officers Liability	Required by a board of directors to protect them in the event they are sued in conjunction with their duties.
Employment Practices Liability	Protects employers against claims made by employees for discrimination (age, sex, race, disability, etc.), wrongful termination, and sexual harassment.
Business Interruption	Physical damage is not the only consideration when determining potential disaster scenarios. An organization should also include death, disability or kidnapping of key personnel; Defection of key personnel to a competitor; Theft of Trade Secrets; Image Management (public perception).
Kidnap/Ransom & Extortion Coverage (see Business Interruption)	Provides coverage for kidnappings and other events through a combination of financial indemnification and expert crisis management.
Group Personal Liability	Coverage for key personnel, managers, and employees.
Key Person Life Coverage	This coverage is designed to protect your business upon the loss of a key employee. The tax-free proceeds from this policy can be used to find, hire and train a replacement, compensate for lost business during the transition, or finance any number of timely business transactions (typically found in US policy structure).
Media Liability Coverage	Protects you against claims arising out of the gathering and communication of information. Media Liability Insurance provides very valuable coverage against defamation and invasion of privacy claims as well as copyright and/or Trademark infringement. (investigate and clarify the level of privacy coverage before acquisition).
Fidelity or Crime Liability	Protects organizations from loss of money, securities, or inventory resulting from crime.
Network Security Coverage	Protects you from losses associated with unauthorized access to or theft of your data or e-business activities, computer viruses, denial of service attacks, as well as alleged unauthorized e-commerce transactions.
Intellectual Property	Protects companies for copyright, trademark or patent infringement claims arising out of the company's operation. Items such as all working papers, records, trade secrets, data, methodologies, drawings, software, documents or other writings created, developed or acquired the company. This includes any documents, records, trade secrets, data, drawings, software or other writings created by or supplied to or made available the company.
Patent Coverage	A policy which reimburses the insured for defense expenses and damages paid by the insured resulting from allegations that the insured has infringed on a patent, copyright or trademark of a third party.
Workplace Violence coverage (see Business Interruption)	Protection against the expenses that a company can face resulting from incidences of workplace violence, including the cost to hire independent security consultants and public relations experts, as well as payment of death benefits and business interruption expenses.

Figura 2 - *Tipologias de incidentes informáticos e respetivas descrições.*

Fonte: *(Drouin, 2004).*

9. Apêndice

9.1. APÊNDICE 1 - Tabela resumo dos principais diplomas paralelos ao direito dos seguros e à temática em análise

Tabela V *- Tabela resumo - compilação principais diplomas paralelos.*

Diploma	O que regula	Principais artigos	Resumo interpretativo da lei
Dec. Lei nº 12/2006, de 20 de janeiro - DR 1ª Série - A , de 20 Janeiro de 2006	• Regula a constituição e o funcionamento dos fundos de pensões e das entidades gestoras de fundos de pensões; • Regula a gestão transfronteiriça de planos de pensões, quer por entidades nacionais quer por entidades de outros Estados membros	Artsº 1 ,4, 16, 18 , 20 e 33 ; Arts.º 18º, nº1 ; 20º, nº1 e art. 85º nº 1	Menciona aspetos intrínsecos da ligação e partilha de informação entre empresas de seguros e entidades de fundos de pensões; prevê a regulação de matéria da disponibilização de informação, em alinhamento com o regime dos produtos seguradores similares, como é o caso do *"unit-linked."*; Fala de competências e deveres do ISP e transferência de riscos ; Prevê ainda a aceitação de entidades com estabelecimento na União Europeia como entidades depositárias dos fundos de pensões; Em matéria organizacional e estruturas de governação instituem-se regras sobre conflitos de interesse, gestão de riscos e controlo interno das entidades gestoras de fundos de pensões.
Decreto-Lei n.º 94-B/98, de 17 de abril - DR n.º 90/1998, 2º Suplemento, Série I-A de 1998-04-17	Regula as condições de acesso e de exercício da actividade seguradora e resseguradora no território da Comunidade Europeia, incluindo a exercida no âmbito institucional das zonas francas	Artsº 81 a 87	Define as entidades que podem exercer a atividade seguradora (e resseguradora), e respetivas autorizações e conidções de exercício da atiivdade ; Aplica-se ainda ao acesso e exercício da actividade seguradora e resseguradora no território de Estados não membros da União Europeia por sucursais de empresas de seguros ou de resseguros com sede em Portugal, e vice-versa ; Determinação, definição e cálculo de provisões técnicas ; Especifica a determinação de margem de solvências.
Lei nº 147/2015 de 9 de Setembro – DR, 1ª série – Nº176 – 9 de Setembro de 2015	Aprova o **Regime jurídico de acesso e exercício da atividade seguradora e resseguradora;** Aprova o regime processual aplicável aos crimes especiais do setor segurador e dos fundos de pensões e às contraordenações cujo processamento compete à ASF	Arts.º 1, 2 , 10 e 24 do diploma; Arts.º 7,8,32,34, 45 nº6, 72,155, 336 e ss, 256 e ss, e 359 ; Destaca-se o art.8, j) onde se insere o objeto base da nossa investigação - seguros informáticos	• Define as entidades que podem exercer a actividade em Portugal e fornece também algumas definições pertinentes para o enquadramento, como sejam relativas a riscos, empresas de seguros e estados membros onde se situa o risco. • Fala de questões fiscais, princípios, disposições gerais relativas a supervisão, registos, condições de acesso à actividade seguradora e resseguradora por empresas de seguros, códigos de conduta, informação a prestar à ASF, margem de risco, provisões técnicas, capitais, condutas de mercado, gestão de reclamações, fusão ou cisão de empresas de seguros/resseguros, transferências de carteiras, contratos, sanções e incumprimentos, bem como prestações de serviços noutros Estados- Membros. aborda ainda operações intra grupo, medidas de recuperação, dimensões transfronteiras, ilícitos penais e contra-ordenação pervistas, etc
Lei nº 148/2015 de 9 de Setembro , DR n.º 176/2015, Série I de 2015-09-09	Aprova o Regime Jurídico da Supervisão de Auditoria; assegura a execução, na ordem jurídica interna, do Regulamento (UE) n.º 537/2014, do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativo aos requisitos específicos para a revisão legal de contas das entidades de interesse público	Arts.º 1,5, 35 e 37	Grande parte de legislação está apenas relacionada com a actividade regulatória de supervisão de fundos de pensões, e com a fiscalização de entidades de interesse público, o que não se considera pertinaz mencionar no contorno desta investigação.
Diretiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009	Relativa ao acesso à atividade de seguros, resseguros e ao seu exercício	Arts.º 153 a 157; Arts. º 178, 179 e 183. Anexo I - Ramos de Seguro não Vida , nº9	Alude à necessidade de proporcionar um enquadramento legal às empresas de seguros e de resseguros, para o exercício da actividade em todo o mercado interno, de forma a facilitar às empresas de seguros e de resseguros, com sede na Comunidade, a cobertura de riscos e compromissos nela situados; Ambiciona fixar regras coordenadas, relativas à supervisão dos grupos seguradores e garantir a protecção dos credores, aos processos de saneamento e de liquidação das empresas de seguros. Pretende também assegurar a harmonização necessária e suficiente para garantir o reconhecimento mútuo das autorizações e dos sistemas de supervisão, de modo a criar uma autorização única, válida em toda a Comunidade, e possibilitar a supervisão da empresa pelo Estado-Membro de origem. Adoptar uma abordagem económica baseada no risco.
Portaria n.º 74-B/2016 - DR, 2.ª série — N.º 59 — 24 de março de 2016	Fixa as taxas devidas à Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) pelas empresas de seguros, entidades gestoras de fundos de pensões, mediadores de seguros ou de resseguros e entidades promotoras de cursos de formação sobre seguros.	Arts.º 1 e 3 ; Art. 3º e ss	Concretiza o disposto no n.º 2 do artigo 38.º dos Estatutos da ASF e no n.º 3 do artigo 34.º da Lei-Quadro das entidades reguladoras; Introduz novos termos conexos: **APFIPP** — Associação Portuguesa de Fundos de Investimento, Pensões e Patrimónios e APROSE — Associação Nacional de Agentes e Corretores de Seguros.

Legenda: Síntese dos principais regulamentos, diretivas e diplomas que se cruzam com a presente investigação, embora de forma acessória (Parte 1).
Fonte: Própria.

Diploma	O que regula	Principais artigos	Resumo interpretativo da lei
Regulamento (UE) N.o 1094/2010 do Parlamento Europeu e do Conselho de 24 de Novembro de 2010	O presente regulamento cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Seguros e Pensões Complementares de Reforma) - EIOPA	Artsº 1 , 6 , 18, 27, 32 e 37.	Nos termos deste Regulamento, a ASF coopera com a EIOPA (Autoridade) para os efeitos previstos no RJARSR, e presta à mesma, de forma atempada, a informação sistemática ou pontual necessária à execução das funções que lhe são conferidas ao longo do presente; A Autoridade deverá agir com vista a melhorar o funcionamento do mercado interno, nomeadamente através de um nível elevado, eficaz e coerente de regulação e supervisão, tomando em consideração os interesses de todos os Estados-Membros e a natureza diversa das instituições financeiras. Deverá também proteger valores públicos como a transparência dos mercados e a protecção dos tomadores de seguros; Refere ainda que no sector dos seguros, é de realçar também a intenção da Comissão de analisar a possibilidade de introduzir regras da União que protejam os titulares de seguros no caso de falência de uma companhia de seguros. A Autoridade coopera regular e estreitamente com o ESRB - Comité Europeu do Risco Sistémico.
Decreto-Lei n.º 72/2008 de 16 de Abril - Diário da República, 1.ª série — N.º 75	**Aprova o Regime Jurídico do Contrato Seguro**	Arts.º 1 , 3 , 5 ,11, 14, 15, 16, 22, 24 , 30 , 37,43,44,45,49, 50, 51 e ss , 62, 72, 91,93,99,100, 122,123, 126, 133,137,192 e 193. Arts.º 21º, nº5 e 32, nº 2	Este diploma consolida o regime geral do contrato seguro para evitar fragmentação e dispersão legislativa, facilitando o conhecimento do regime para os operadores; Reconhece a necessidade da alteração de paradigma liberal da legislação, e a necessidade da parte contratual mais débil; Esta reforma vem adaptar as regras em vigor, procedendo à actualização e concatenação de conceitos de diversos diplomas e preenchendo certas lacuna; Regula alguns casos omissos na actual legislação e introduz diversas soluções normativas inovadoras; Atende também a um conjunto de desenvolvimentos no âmbito dos seguros de responsabilidade civil; Aborda questões cruciais em matéria do risco, declaração inicial do risco; Fala dos direitos e deveres tanto do segurador como do tomador do seguro;
Lei nº 144/2015 , DR n.º 175/2015, Série I de 2015-09-08	Estabelece o enquadramento jurídico dos mecanismos de resolução extrajudicial de litígios de consumo;	Arts.º 1, 2, 3 a) , 4 , 5 , 10 e 15	Aplicável aos procedimentos de resolução extrajudicial de litígios nacionais e transfronteiriços promovidos por uma entidade de resolução alternativa de litígios (RAL); Cooperação entre as entidades de resolução alternativa de litígios; Procedimentos de resolução alternativa de litígios , e menciona também deveres de informação e cooperação
Lei n.º 63/2011, de 14 de Dezembro - DR n.º 238/2011, Série I de 2011-12-1	Aprova a Lei da Arbitragem Voluntária	Arts.º 1 , 30 , 39, 49 e ss	Desde que por lei especial não esteja submetido exclusivamente aos tribunais do Estado ou a arbitragem necessária, qualquer litígio respeitante a interesses de natureza patrimonial pode ser cometido pelas partes, mediante convenção de arbitragem, à decisão de árbitros; A convenção de arbitragem pode ter por objecto um litígio actual, ainda que afecto a um tribunal do Estado (compromisso arbitral), ou litígios eventuais emergentes de determinada relação jurídica contratual ou extracontratual; Esclarece e submete a arbitragem questões de natureza contenciosa, e que requeiram a intervenção de um decisor imparcial; Define e enumera os princípios e regras do processo arbitral.
Lei n.º 29/2013 de 19 de abril - DR, 1.ª série — N.º 77 — 19 de abril de 2013	Estabelece os princípios gerais aplicáveis à mediação realizada em Portugal, bem como os regimes jurídicos da mediação civil e comercial, dos mediadores e da mediação pública	Arts.º 1, 2 , 10 , 38 , 3 e ss	Enumera os vários princípios da atividade de mediação civil, quer de conflitos, bem como os procedimentos e fiscalização desta atividade
Diretiva sobre Distribuição de Seguros	Implicou uma revisão substancial do Dec. Lei nº 144/2006 de 31 de julho.	Transposta para o ordenamento jurídico nacional em Fevereiro de 2018	Este diploma relaciona-se com a necessidade de garantir aos consumidores o mesmo nível de protecção, independentemente do facto de existirem diferentes canais de distribuição de seguros

Legenda: Idem (Parte 2).
Fonte: Própria

9.2. APÊNDICE 2 - CheckRisk Framework.

Tabela VI– *Check Risk Framework - modelo de apresentação.*

Nível tolerância ao Risco /Taxonomia de Riscos Operacionais	Ações de Pessoas	Sistemas e Tecnologias	Processos Internos	Eventos Externos
Intolerante (1-3)	X			
Pouco Tolerante (4-6)			X	X
Tolerante (7-9)		X		

Legenda: Framework construída para análise de risco informático (modelo exemplificativo de apresentação).
Fonte: Própria. Adaptado de (Cebula, J & Young, L. (2010)., Eling, M. & Wirfs, J. H. (2015). e NIST (2017).

Tabela VII *- Check Risk Framework – modelo explicativo.*

Nível tolerância ao Risco /Taxonomia de Riscos Operacionais	Ações de Pessoas	Sistemas e Tecnologias	Processos Internos	Eventos Externos
Intolerante (1-3)	A	D	G	J
Pouco Tolerante (4-6)	B	E	H	K
Tolerante (7-9)	C	F	I	L

Legenda: Framework construída para análise de risco informático (modelo detalhado/explicativo).
Fonte: Própria. Adaptado de ITSO (2007). Cebula, J & Young, L. (2010), Biener, C. et al. (2015) e ACS, (2016).)

***Tabela VIII**- Justificação para escolha de quadrante.*

Letra	SIGNIFICADO/JUSTIFICAÇÃO DA ESCOLHA -QUADRANTE CORRESPONDENTE PARA SELEÇÃO DA POSIÇÃO NO FRAMEWORK
A	Certo tipo de erros, vandalismos, omissões, furtos, sabotagens, falta de conhecimento, disponibilidade ou orientação do mapa de pessoal da sua empresa (ou outras pessoas que interagem com a mesma), podem levar a desfechos, modificações, destruições ou disrupções *severas ou catastróficas. Os vetores e agentes do risco apresentam-se enquanto ameaça alta.*
B	Certo tipo de erros, vandalismos, omissões, furtos, sabotagens, falta de conhecimento, disponibilidade ou orientação do mapa de pessoal da sua empresa (ou outras pessoas que interagem com a mesma), podem levar a desfechos, modificações, destruições ou disrupções *com graves consequências ou efeitos adversos/críticos. Os vetores e agentes do risco apresentam-se enquanto ameaça a nível médio.*
C	Certo tipo de erros, vandalismos, omissões, furtos, sabotagens, falta de conhecimento, disponibilidade ou orientação do mapa de pessoal da sua empresa (ou outras pessoas que interagem com a mesma), podem levar a desfechos, modificações, destruições ou disrupções *com efeitos adversos controláveis ou consequências limitadas. Os vetores e agentes do risco apresentam-se enquanto ameaça baixa.*
D	Falhas relacionadas com compatibilidade/gestão de configurações de segurança, práticas, testes e controlos de rede, bem como especificações, design e complexidade de sistemas ou equipamentos podem culminar em desfechos, modificações, destruições ou disrupções *severas ou catastróficas para a minha empresa. Os vetores e agentes do risco apresentam-se enquanto ameaça alta.*
E	Falhas relacionadas com compatibilidade/gestão de configurações de segurança, práticas, testes e controlos de rede, bem como especificações, design e complexidade de sistemas ou equipamentos podem culminar em desfechos, modificações, destruições ou disrupções *graves ou com efeitos adversos/críticos para a minha empresa. Os vetores e agentes do risco apresentam-se enquanto ameaça a nível médio.*
F	Falhas relacionadas com compatibilidade/gestão de configurações de segurança, práticas, testes e controlos de rede, bem como especificações, design e complexidade de sistemas ou equipamentos podem culminar em desfechos, modificações, destruições ou disrupções *adversas, controláveis e de efeito limitado para a minha empresa. Os vetores e agentes do risco apresentam-se enquanto ameaça baixa.*
G	Falhas a nível de documentação, fluxo de processos, funções, responsabilidades, notificações, informações ou alertas, bem como problemas em acordos de nível de serviço, monitorização de tarefas, revisões periódicas, aquisições, desenvolvimento, formação, pessoal ou contabilidade podem culminar em desfechos, modificações, destruições ou disrupções *severas ou catastróficas para a minha empresa. Os vetores e agentes do risco apresentam-se enquanto ameaça alta.*
H	Falhas a nível de documentação, fluxo de processos, funções, responsabilidades, notificações, informações ou alertas, bem como problemas em acordos de nível de serviço, monitorização de tarefas, revisões periódicas, aquisições, desenvolvimento, formação, pessoal ou contabilidade podem levar a desfechos, modificações, destruições ou disrupções com *graves consequências ou efeitos adversos/críticos. Os vetores e agentes do risco apresentam-se enquanto ameaça a nível médio.*
I	Falhas a nível de documentação, fluxo de processos, funções, responsabilidades, notificações, informações ou alertas, bem como problemas em acordos de nível de serviço, monitorização de tarefas, revisões periódicas, aquisições, desenvolvimento, formação, pessoal ou contabilidade podem levar a desfechos, modificações, destruições ou disrupções *com efeitos adversos controláveis ou consequências limitadas. Os vetores e agentes do risco apresentam-se enquanto ameaça baixa.*
J	Sempre que derivado de qualquer tipo de catástrofe natural, falha de energia, condições económicas (ou de mercado), irregularidades no fornecimento, produção, transportes, serviços públicos ou de emergência, bem como inconformidades regulamentares, legais ou outros litígios de fonte/origem externa, produzam desfechos, modificações, destruições ou disrupções *severas ou catastróficas. Os vetores e agentes do risco apresentam-se enquanto ameaça alta.*
K	Sempre que derivado de qualquer tipo de catástrofe natural, falha de energia, condições económicas (ou de mercado), irregularidades no fornecimento, produção, transportes, serviços públicos ou de emergência, bem como inconformidades regulamentares, legais ou outros litígios de fonte/origem externa, produzam desfechos, modificações, destruições ou disrupções *graves ou com efeitos adversos/críticos para a minha empresa. Os vetores e agentes do risco apresentam-se enquanto ameaça a nível médio.*
L	Sempre que derivado de qualquer tipo de catástrofe natural, falha de energia, condições económicas (ou de mercado), irregularidades no fornecimento, produção, transportes, serviços públicos ou de emergência, bem como inconformidades regulamentares, legais ou outros litígios de fonte/origem externa, produzam desfechos, modificações, destruições ou disrupções *com efeitos adversos controláveis ou consequências limitadas. Os vetores e agentes do risco apresentam-se enquanto ameaça baixa.*

Legenda: Cruzamento com grelha de vulnerabilidade de informações (próprias ou de terceiros) e onde auxilia a empresa alvo desta framework a selecionar uma letra por coluna, consoante a posição da sua empresa ao exposto. Na presente tabela explana-se as justificações e detalhes atribuídos a cada letra, consoante a opção mais enquadrada do cliente. **Fonte:** Própria. Adaptado de (ITSO (2007). Cebula, J & Young, L. (2010),Biener, C. et al. (2015) e ACS, (2016).

***Tabela IX** - Justificação para escolha de escala quantitativa.*

CORRESPONDÊNCIA PONTUAÇÃO	NÍVEL TOLERÂNCIA SELECIONADO	JUSTIFICAÇÃO/ENQUADRAMENTO
1 a 3 (Intolerante)	**1**	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) resulte *numa interrupção de uso ou acesso (temporário/permanente) a informações* com impacto severo sobre operações, ativos ou indivíduos da organização.
	2	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) resulte *numa modificação, extração ou destruição de informações* com impacto severo sobre operações, ativos ou indivíduos da organização.
	3	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) resulte *numa exposição, disseminação ou divulgação não autorizada de informações* com impacto severo sobre operações, ativos ou indivíduos da organização.
4 a 6 (Pouco Tolerante)	**4**	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) *resulte numa interrupção de uso ou acesso (temporário/permanente) a informações* com impacto grave sobre operações, ativos ou indivíduos da organização.
	5	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) *resulte numa modificação, extração ou destruição de informações* com impacto grave sobre operações, ativos ou indivíduos da organização.
	6	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) *resulte numa exposição, disseminação ou divulgação não autorizada de informações* com impacto grave sobre operações, ativos ou indivíduos da organização.
7 a 9 (Tolerante)	**7**	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) resulte *numa interrupção de uso ou acesso (temporário/permanente) a informações* com impacto limitado sobre operações, ativos ou indivíduos da organização.
	8	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) resulte *numa modificação, extração ou destruição de informações com impacto* limitado sobre operações, ativos ou indivíduos da organização.
	9	Quando se espera que a verificação/consumação do fator de risco (na respetiva coluna de análise) resulte *numa exposição, disseminação ou divulgação não autorizada de informações* com impacto limitado sobre operações, ativos ou indivíduos da organização.

Legenda: Detalhe da pontuação a atribuir, paralelamente à escolha de um nível de tolerância. – Tabela Resumo. Define para que serve cada número, e como funciona a métrica quantitativa em paralelo com a qualitativa. Por cada linha de análise/escolha, haverá a selecionar um número apenas, sendo aquele mais adequado à descrição e empresa alvo.
Fonte: Própria. Adaptado de (ITSO (2007). Cebula, J & Young, L. (2010),Biener, C. et al. (2015) e ACS, (2016).

9.3. APÊNDICE 3 - Figuras várias – complementares e explicativas.

Tabela X *- Principais elementos na gestão de riscos empresariais*

Elementos Chave para gestão de riscos empresariais
Ambiente Interno (cultura de risco, compromisso de competência, integridade e valores éticos, estrutura da organização, políticas e práticas em matéria de recursos humanos)
Estabelecimento de objetivos (objetivos estratégicos, tolerância ao risco, risco "aceitável")
Identificação de acontecimentos (fatores de influência estratégica e de objetivos, acontecimento interdependentes, riscos e oportunidades)
Avaliação de riscos (probabilidade e impacto, risco inerente e residual, fontes de dados técnicos de avaliação, correlação entre acontecimentos)
Resposta aos riscos (avaliação de possíveis respostas, seleção de respostas)
Atividades de controlo (integração da resposta ao risco, tipos de atividades de controlo, controlo dos sistemas de informação e controlos específicos da entidade)
Informação e comunicação (análise e triagem de procedimentos, com respetivos controlos)
Supervisão (comunicação de deficiências, avaliações independentes, atividades permanentes de supervisão/coordenação).

Legenda: Compilação dos principais elementos a ter em atenção numa gestão de riscos em empresas, com sucinta explicação de cada um deles. **Fonte:** Própria. Adaptado de (San José-Marti, 2013).

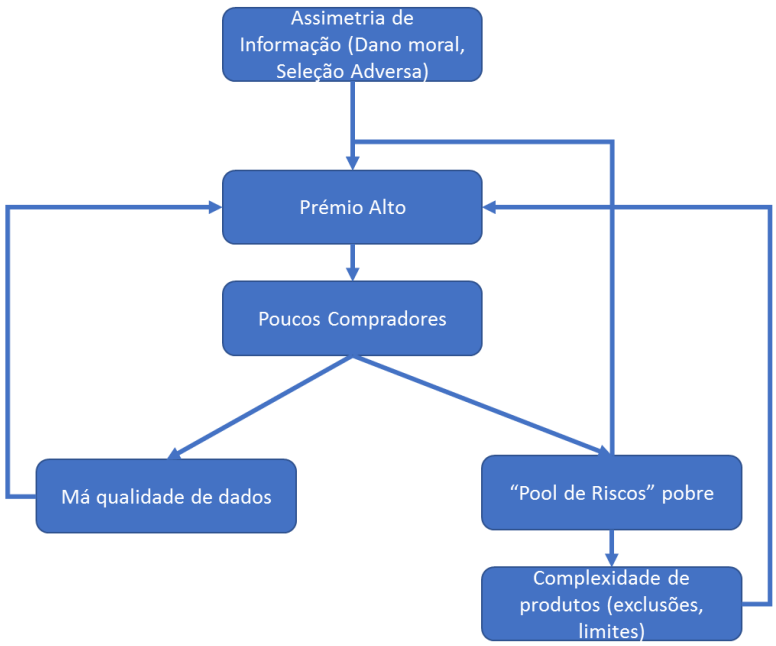


Figura 3- *Esquema resumo dos principais problemas com o seguro informático.*

Fonte: *Própria. Adaptado de (Kesan & Zhang, 2016).*

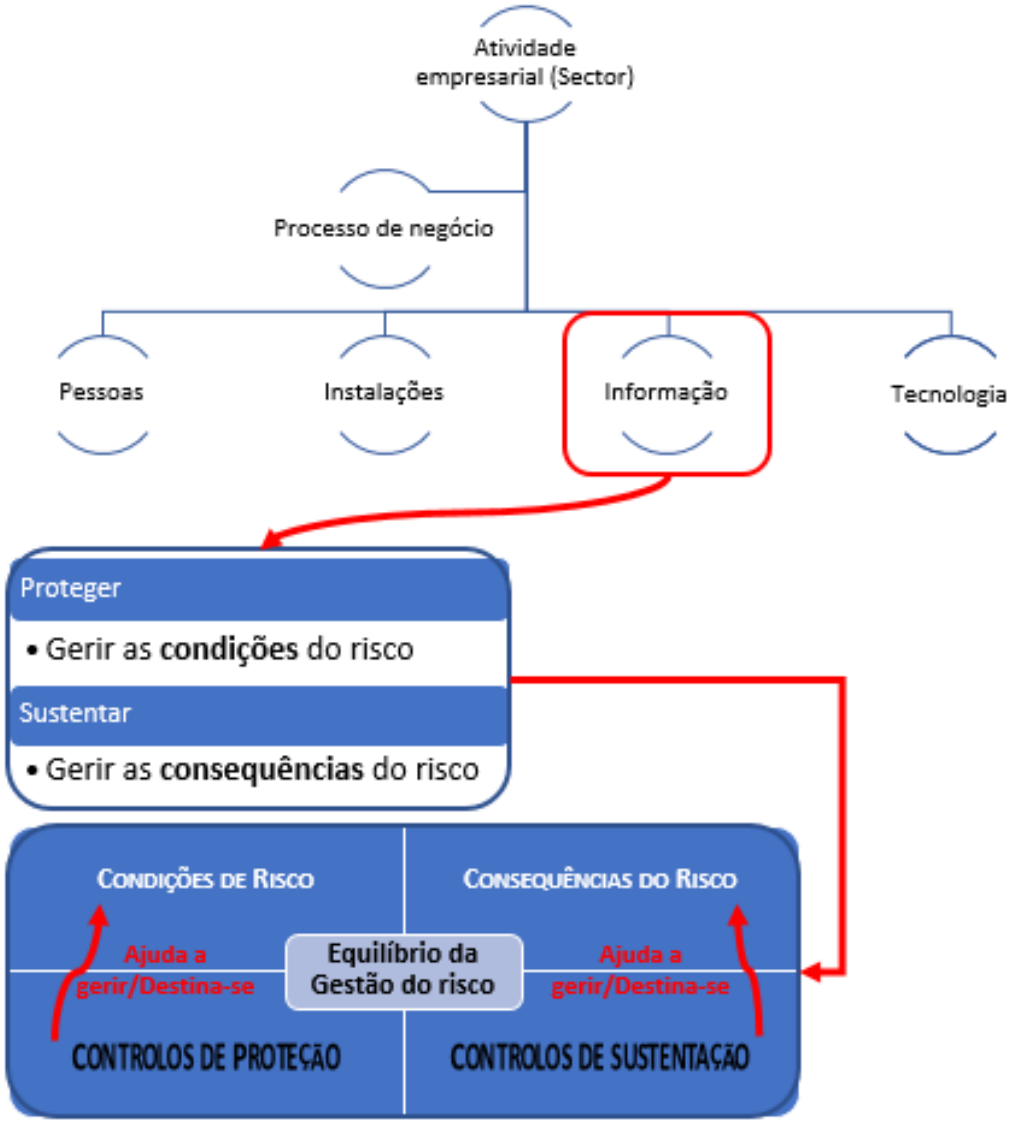


Figura 4 - *Esquema representativo para um equilíbrio do risco.*

Diagrama sequencial onde se destacam os principais ativos enquanto unidades base de valor numa organização, sendo os blocos de construção de um processo de negócio. Especial destaque para a informação enquanto ativo crítico nos riscos operacionais.
Fonte: *Própria. Adaptado de Cebula, J. & Young, L. (2010).*

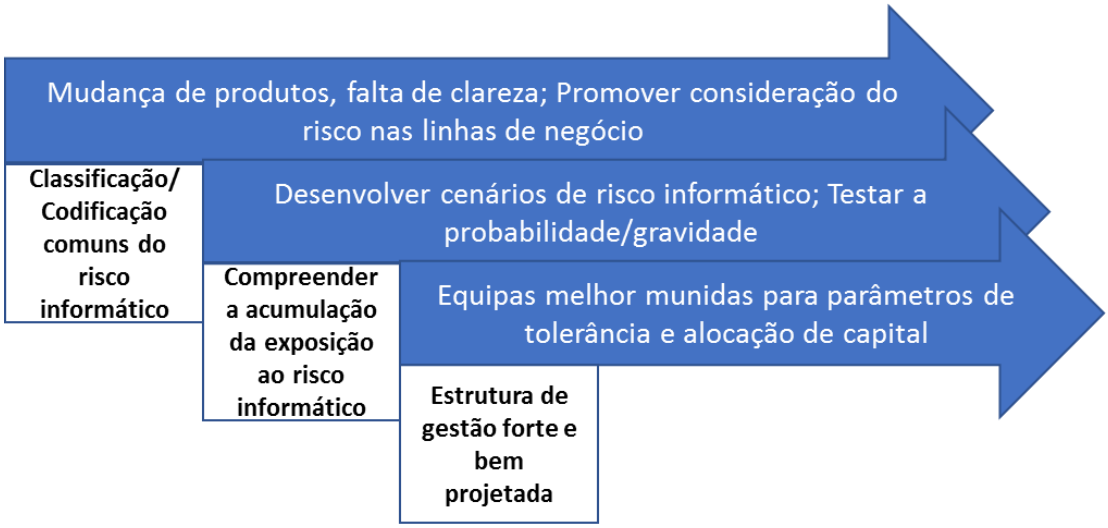


Figura 5 *- Processo para entendimento comum do risco.*

Exemplo de processo a adotar por empresas na perspetiva da gestão de risco e resiliência informática. ***Fonte:*** *Própria. Adaptado de Kitching, N. et. Al (2014).*

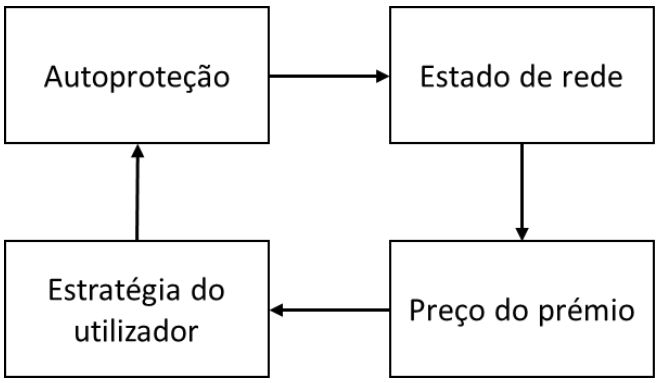


Figura 6 *- Ciclo de feedback de segurança na rede*

Através da análise deste esquema é possível avaliar o impato de fatores externos e dos utilizadores, com e sem seguro em vigor, o que auxilia na busca de soluções de segurança para proteção contra riscos informáticos. ***Fonte:*** *Própria. Adaptado de Bolot, J & Lelarge, M. (2008).*

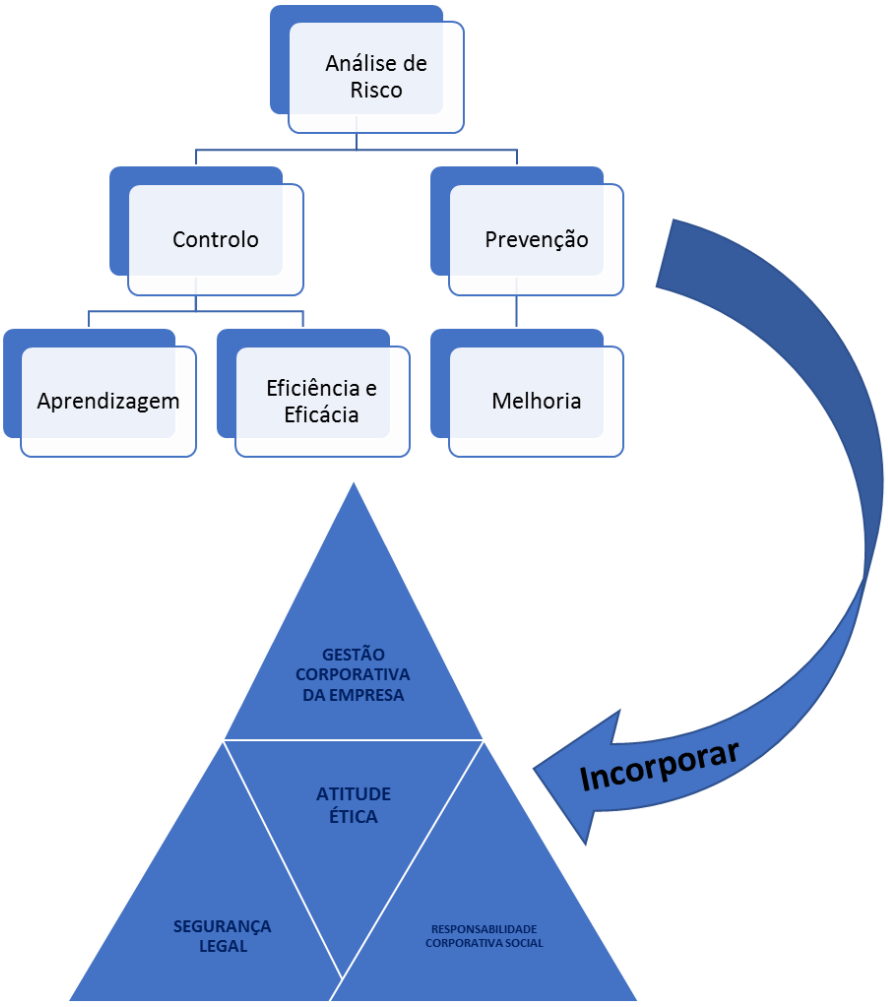


Figura 7 *- Esquema interrelacionado para atualização de mapa de riscos.*

Para uma atualização do mapa de riscos de uma empresa, deve abordar-se a avaliação do risco, o tratamento do risco, a monitorização e revisão do risco (auditoria periódica do plano validado). ***Fonte:*** *Própria. Adaptado de Bonet, A. E. (2012)*

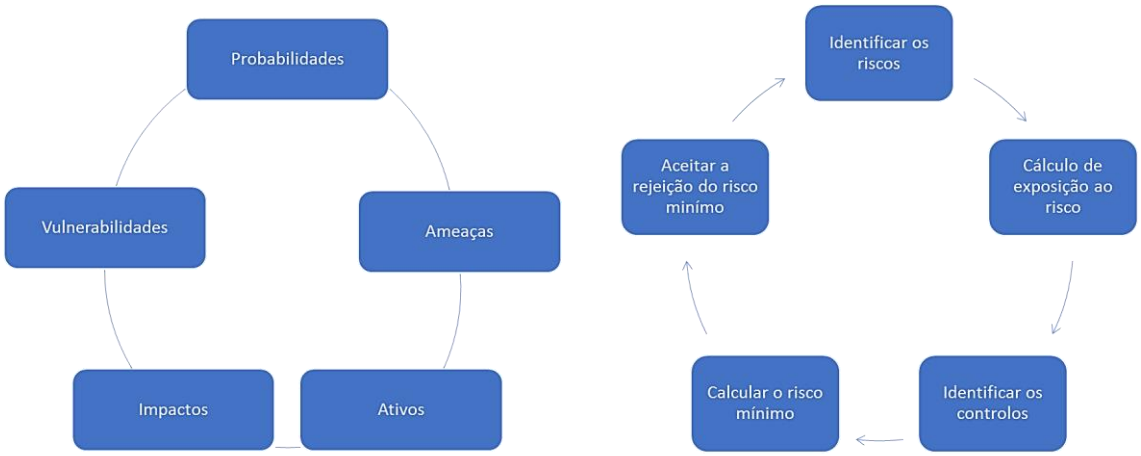


Figura 8 - *Ciclos exemplificativos de mecânicas ao nível do risco.*

Mecânicas para reflexão atendendo ao nível de segurança de uma empresa. Funcionamento de acordo com ferramentas e etapas para minimizar o risco tecnológico. ***Fonte****: Própria. Adaptado de Tenzer, S. M & Sena, L. (2004).*

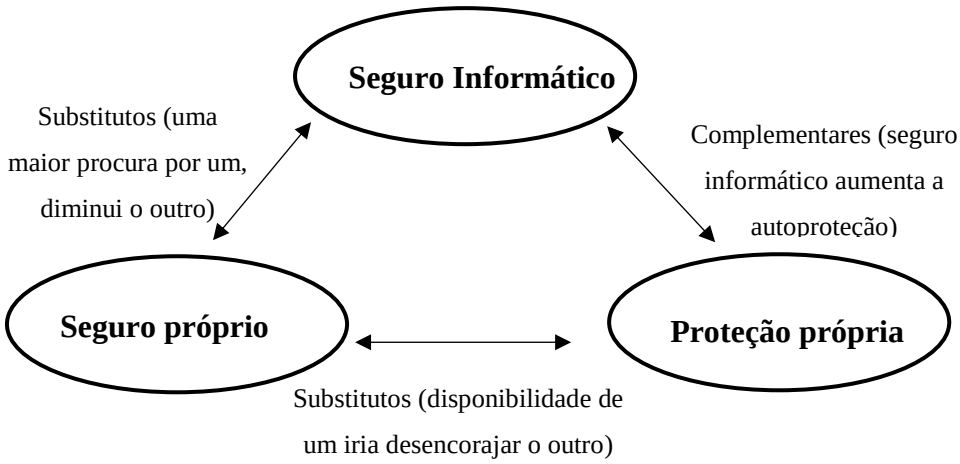


Figura 9 - *Interconetividade de posições em relação ao risco informático.*

Compreende-se a natureza complementar ou substituta das posições empresariais quanto ao risco informático, sendo que a melhor opção será contrair seguro informático apostando numa constante melhoria da proteção própria. ***Fonte:*** *Própria. Adaptado (Cebula & Young, 2010) e (Kesan 2004).*

9.4. APÊNDICE 4 – Conjunto de questionários

	Ação	Sim	Não
	1. TRANSAÇÕES ELETRÓNICAS		
1.1	A sua empresa realiza alguma das suas operações através da Internet?		
1.2	Atendendo à quantidade de crimes informáticos reportados em todo o mundo, considera que sua empresa está em risco neste âmbito?		
1.2.1	Em caso afirmativo: a) a quantos? ; b) de que tipo? ; c) com que potenciais consequências?		
1.3	A sua empresa já foi vítima, reportou ou detetou algum cibercrime ou outros incidentes informáticos?		
1.4	No seio da sua organização acha mais provável ser cometido um crime/ilícito informático a partir de fonte interna ou externa?		
1.5	Considera que o risco informático é suscetível afetar a sua empresa no futuro?		
	2. AVALIAÇÃO DE MEDIDAS PREVENTIVAS IMPLEMENTADAS		
2.1	Existem medidas preventivas implementadas, relativamente aos riscos informáticos?		
2.2	As várias estratégias internas da empresa contra ataques informáticos são descritas na íntegra aos funcionários (em detalhe e com explicação de possíveis cenários, de modo a que os mesmos tenham um conhecimento técnico e noção de reconhecer sinais primários de alguma irregularidade) os reportem e trabalhem ativamente na prevenção desta ameaça?		
2.3	Os funcionários sabem quem, quando e de que forma devem notificar, dentro e fora da empresa, um caso de um eventual ataque/violação de dados?		
2.4	Os funcionários com acesso a sistemas/instalações altamente críticos, recebem códigos de acesso especiais, com rotatividade, e que permitam sinalizar se estão sob coação?		
2.5	Os funcionários sabem como restaurar informações comprometidas nos sistemas para o seu último estado de atualização? E existem mecanismos de recuperação?		
2.6	Os funcionários sabem como isolar sistemas que foram comprometidos e removê-los da rede?		
2.7	Existem canais alternativos de comunicação que podem ser utilizados no caso dos canais normais serem comprometidos, removendo-os da rede?		
2.8	Existem planos para reduzir a contaminação/disseminação de *malware*, ou outros do género?		
2.9	Existem sistemas automatizados de deteção e monitorização que emitiriam alerta para casos remotos ou caso alguma infração estivesse a ser cometida?		
	3. PROSPETO DA APÓLICE DE SEGURO INFORMÁTICO		
3.1	A empresa tem conhecimento do que é uma apólice de seguro informático?		
3.1.1	Tem alguma de momento?		
3.1.2	Se não, estará a empresa disposta a substituir a apólice atual, por uma de índole unicamente informática, se oferecer coberturas/benefícios mais amplos?		
3.2	A empresa tem atualmente uma apólice de seguro que cobre danos em equipamentos informáticos apenas, ou que também contempla outro/todo o tipo de riscos informáticos?		
3.3	A empresa está satisfeita com o funcionamento/nível das coberturas da presente apólice em vigor?		
3.4	Estaria a empresa disposta a pagar um custo um pouco maior do que o prémio na sua apólice atual, por uma apólice de seguro informático com maior cobertura?		

***Figura 10** - Questionário sintético para avaliação do estado de maturação informática.*

Questionário A - permite avaliar a maturidade informática de uma empresa, de modo superficial, consoante certas categorias. Todas as respostas serão de sim ou não. ***Fonte:*** *Própria - Adaptado de (Adeleke, et al. 2011).*

	Questão	Resposta aberta
1.	Qual a quantidade (aproximada) de informações de identificação pessoal que processa a empresa?	
1.1	Quantos registos relacionados com saúde? E de cartões de crédito?	
2	A empresa fornece serviços *online* a terceiros?	
2.1	E comercializa serviços/produtos online (e-commerce)?	
3	A sua empresa avaliou o impato financeiro de uma eventual violação informática da propriedade intelectual e/ou de uma interrupção de serviço de rede/bloqueio de estruturas de TI?	
3.1	A reputação da empresa ficaria comprometida devido a uma violação de dados?	
4.	A sua organização tem um conjunto completo de informações sobre políticas de segurança periodicamente atualizado e comunicado a todos os empregados?	
5.	Considera possível que um *hacker* cometesse um crime informático (fraude, burla informática, outros) que pudesse afetar a sua empresa ou clientes?	
6.	A empresa confia em terceiros para serviços de TI (consultoria externa)?	
7.	Foi alguma vez investigado o potencial de risco informático que possa causar danos a escritórios, instalações ou outros ativos físicos?	
8.	Tem conhecimento de alguma auditoria de conformidade de privacidade e proteção de dados independente, realizada na sua empresa, no último ano?	
8.1	E testes de avaliação de vulnerabilidades, ou testes de penetração?	
8.2	Alguma vez, no último ano, foram feitas avaliações de risco informático com vista a identificar todos os riscos relevantes para o negócio?	
8.3	E certificações de segurança de informação?	
9.	Alguma vez, no último ano, a sua empresa foi vítima de algum tipo de ataque informático?	
9.1	Se sim, foi o mesmo reportado/divulgado? E como foi ultrapassado?	
10.	A empresa tem alguma política de incidentes e gestão de crises que aborde questões de violações de dados e ataques informáticos?	
10.1	E plano de recuperação de desastres, com *backups* e outros semelhantes?	
11.	A rede e *network* da empresa é periodicamente auditada/verificada por terceiros para assegurar a conceção e implementação adequada de tecnologias de segurança?	
12.	São partilhados dados pessoais, frequentemente ou comummente com outras empresas, no decorrer da atividade/negócio em questão?	
13.	São providenciadas pela empresa ações de formação e sensibilização sobre privacidade de dados e segurança para empregados, colaboradores, incluindo sobre responsabilidades legais e questões de engenharia social?	
14.	Existe alguma política/procedimento de classificação da informação consoante a sensibilidade da mesma, incluindo encriptação de dados sensíveis?	
15.	De um modo geral, como se processa a posse física de documentos na sua empresa? E arquivo/vigilância das instalações?	
16.	O regime recentemente instaurado de que retrata o RGPD, encontra-se devidamente em conformidade e implementado na sua empresa?	
17.	Numa escala de 0 a 5 (sendo 0 Extremamente Intolerante e 5 Bastante Tolerante), em que posição coloca a sua empresa em relação a tolerância ao risco informático?	
18.	De entre os Ativos : Ações de Pessoas, Sistemas e Tecnologias, Processos Internos, e Eventos Externos, qual acha que seria o vetor mais provável (frágil) para uma intrusão informática na sua empresa?	
19.	De um modo geral, considera ter uma exposição ao risco informático Baixa, Moderada ou Elevada?	
20.	Colocando a sua empresa numa postura face à segurança informática, proteção de infraestruturas tecnológicas e segurança da informação, diria tratar-se de um: • Iniciante; • Conservador de Segurança; • Inovador Imprudente; ou • Inovador Digital Seguro?	

***Figura 11**- Questionário Standard (Checklist).*

Questionário B - que aborda aspetos pertinentes para entender a exposição, preparação e perceção do/ao risco de uma empresa, atendendo a algumas variáveis que pretendem auxiliar numa matriz de risco. Surge sob a forma de checklist que ***Fonte:*** *Própria. Adaptado de (Noonan, 2011) e (Santiago, 2016).*

	Questão	Resposta aberta
1.	Quais são os critérios com mais impacto através dos quais o risco de um potencial cliente e/ou novo vínculo contratual é avaliado?	
2.	Na eventualidade de submeter uma apólice de seguro informático pretendia que a mesma fosse válida para todos os setores de negócios, ou apenas um conjunto em particular? Se sim, enumere quais (Comunicação, Serviços Financeiros, TI etc).	
3.	A oferta de seguro informático conduziria à mesma avaliação de risco para todos os setores?	
4.	A oferta de seguro informático cobre todos os riscos, ou apenas particularmente alguns? Se em particular, enumerar quais (ameaça interna, extração de dados, violação de dados)	
5.	A oferta de seguro tem um requisito de auditoria. Indique se este será preferencialmente interno ou externo, se necessita de estar acreditado/certificado ou bastará ser realizado por empresas de consultoria, etc.	
6.	A oferta de seguro informático enfrenta desafios em relação à avaliação de risco da empresa?	
6.1	O histórico de incidentes/ameaças de violações informáticas irá espelhar ocorrências anteriores à data de início da apólice, e ditar a probabilidade de futuras intrusões informáticas? Se não, enunciar algumas das medidas a serem tidas ao momento para contributo de resiliência informática na sua organização.	

Figura 12 - *Questionário de enfoque na oferta (seguro informático).*

Questionário C - permite avaliar a perceção e noção do cliente/empresa a esta modalidade de seguro. Ajuda já a circunscrever as coberturas às necessidades do segurado. ***Fonte:*** *Própria - Adaptado de (ENISA, 2016).*

9.5. APÊNDICE 5 – Conjunto de Fluxogramas

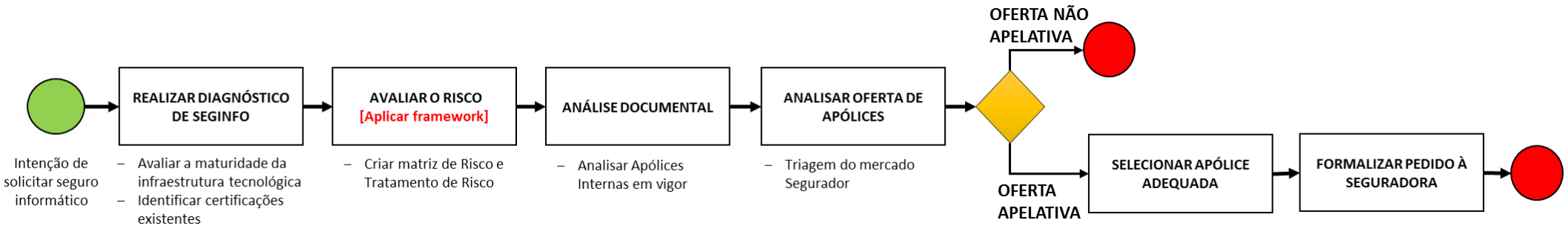
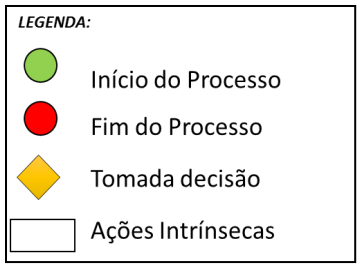


Figura 13 - *Client-Reaches-Insurer Workflow (Fase 1).*

Decisão sobre contrato de seguro informático. Fluxograma representativo do processo de pedido de seguro informático por parte da empresa/cliente. ***Fonte:*** *Própria.*



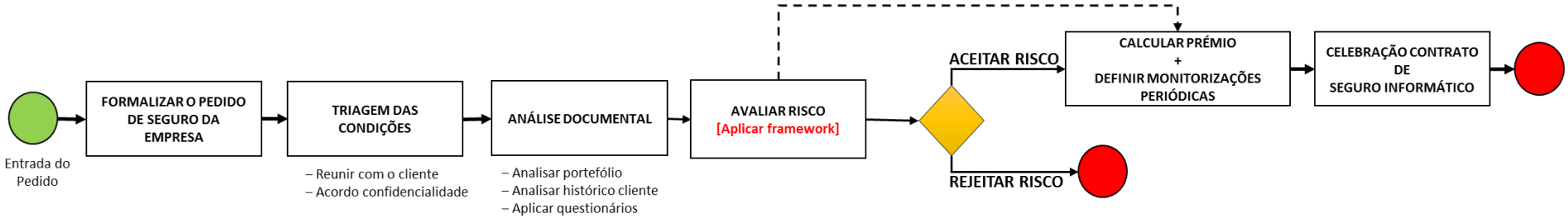
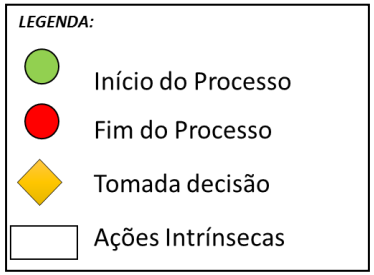


Figura 14 - *Insurance-Request-Processing Workflow (Fase 2).*

Pedido de seguro informático. Fluxograma representativo do processo de pedido de seguro informático, desde que dá entrada na entidade seguradora. ***Fonte:*** *Própria.*



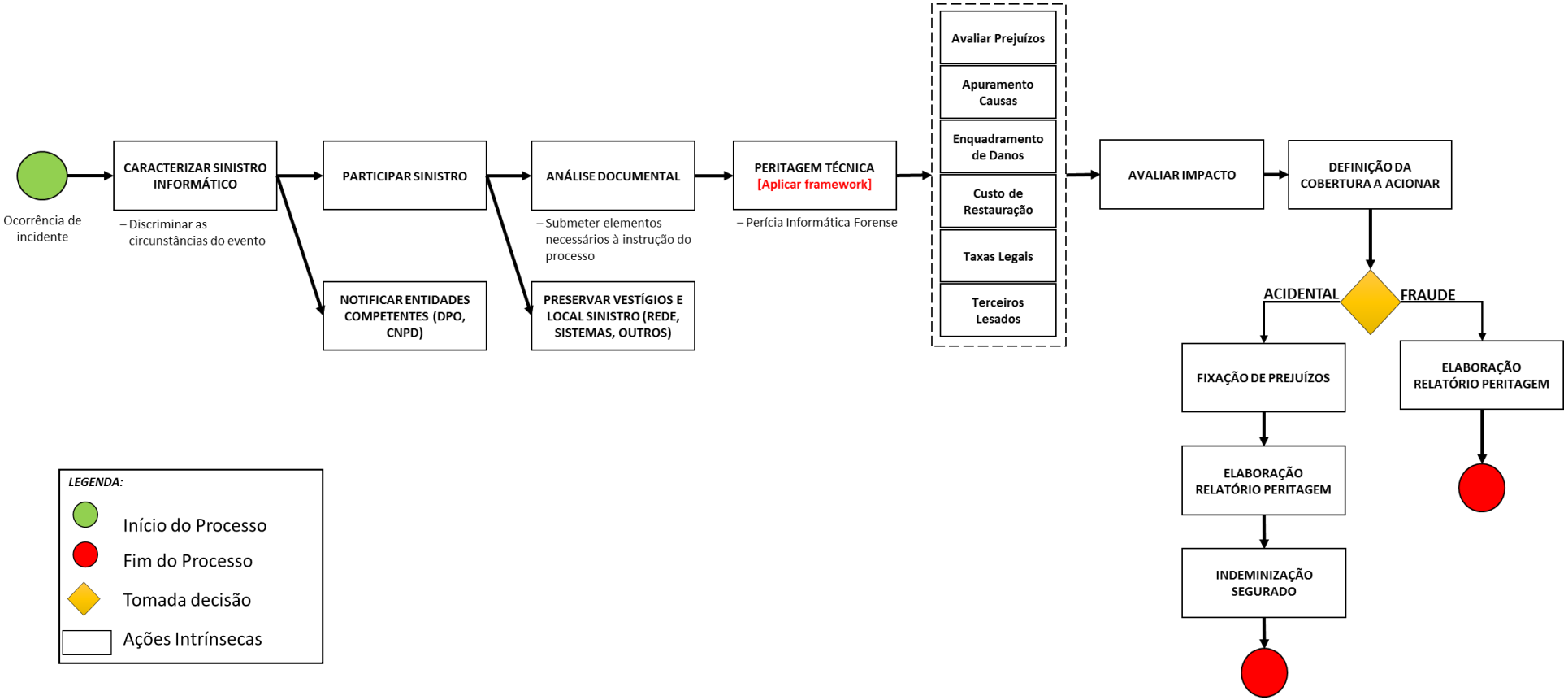


Figura 15 - *Claim-Adjustment Workflow (Fase 3)*

Tratamento de sinistro informático. Fluxograma representativo do processo de participação de sinistro e procedimentos sugeridos após incidente, nomeadamente transmissão à companhia de seguros e etapas seguinte. ***Fonte:*** *Própria.*